Ministerstwo Finansów

ANNEX NO 3
TERRORISM FINANCING RISK SCENARIOS

1. Area – banking

Table no. 1

Type of services, financial products used	bank account
General risk description	usage of the account to collect and transfer money for purposes of terrorist activity
Risk emergence scenario (e. g. possible example of the emergence of risk)	1. Collecting in the bank account of resources obtained in diverse ways (from both legal as well as illegal sources), for the purpose of their payout in cash (frequently in countries bordering countries, in which terrorist activities are active) or further transfers, in most cases to accounts with credit institutions in jurisdictions not adhering to international standards and recommendations from the area of anti-money laundering and combating the financing of terrorism (AML/CTF). 2. Transferring assets from a company controlled by sympathisers with a terrorist organisation, which subsequently announces its bankruptcy. The assets, in this case cash resources, are transferred via a chain of bank accounts belonging to related business entities for the purpose of their payout in cash. 3. Usage of bank accounts of natural persons related to terrorists (families and other next of kin) in order to make cash deposits and afterwards cross-border transfers. 4. Opening of bank accounts for foreign legal entities (registered in particular in tax havens), and then using these bank accounts to transfer resources for the benefit of economic entities found in the area of increased activity of terrorist organisations. 5. Opening of bank accounts by natural persons using counterfeit identity cards. Using bank accounts to transfer funds to persons connected to terrorist activity. 6. Self-financing of terrorists (in particular of so-called "lone wolves") using own resources collected in a bank account (frequently from legal sources – employment, loans/credits, grants, family donations). 7. Transfer of resources for the purposes of terrorist activity from a bank located in Asia to a bank account with a financial institution in Europe. The account would belong to a member or sympathiser of a terrorist organisation or an entity controlled by them, and the resources are transferred via correspondent banks located in South America, hindering the identification and verification of data of the transfer originator . 8. Usage of a bank account by an entity whose beneficial owner is a person found on international lists of sanctions or related to a terrorist organisation or sympathising with it.
Vulnerability level	2

Vulnerability level substantiation	It is relatively easy to open a bank account and make transactions – including international ones – with its use. Significant is access to the account by electronic communication channels (the Internet in particular), as it provides certain capacity to hide the data of actual transaction originators – with the use of so-called straw men or shell companies to open the account. Pursuant to the study of the National Bank of Poland (NBP) entitled *Comparison of selected components of the Polish payment system with the systems of other EU countries for the year 2017*, the number of bank accounts in Poland continues to rise (in the year 2017 it increased as compared to data for 2016 by over 6.6%, meaning, by 4.5 m accounts).[1] The total number per inhabitant is 1.9 and is higher than the current value for the European Union (UE)[2]. Similarly, the total number of transactions made by payment cards, cheques, payment orders and transfers amounted to over 6.51 billion in the year 2017.[3] It must be considered that in terms of transfer orders per capita, Poland is above the EU average, and in terms of payment orders per capita – way below the EU average. All entities offering the above described products/services are obliged institutions (OI). These entities apply customer due diligence measures, even though shortcomings in this area continue to be revealed during audits. They are aware of their obligations in terms of AML/CTF.[4] They analyse transactions efficiently – the most STR[5]/SAR[6] transferred to the General Inspector of Financial Information (GIFI), originate from banks branches of credit institutions/branches of foreign banks (in the year 2017, this was ca. 94.9% SARs from OI and ca. 97.8% STRs). Public administration authorities have knowledge about the risk of money laundering and terrorism financing (ML/TF) in this regard. The GIFI is able to collect and analyse information. There exists the probability that a case of TF is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of domestic and international cooperation of public administration bodies is relatively good. Existing legal provisions correspond mostly to the scope of the analysed risk.
Threat level	4

1 Comparison of selected components of the Polish payment system with the systems of other EU countries for the year 2017, NBP, December 2018, p. 7, at: https://www.nbp.pl/home.aspx?f=/systemplatniczy/obrot_bezgotowkowy/obrot_bezgotowkowy.html.

2 Ibidem, p. 8.

3 Ibidem, p. 32.

4 However, all audits carried out in the year 2018 by the Polish Financial Supervision Authority (e. g. at 12 commercial banks and three cooperative banks) revealed irregularities and divergences in the analysed areas (mainly spanning risk assessment and application of customer due diligence measures, as well as the organisation of the process of countering money laundering and terrorism financing and the transfer of information to the GIFI). The GIFI in turn during four out of five bank audits conducted in the years 2017-2018 revealed irregularities in the execution of obligations in terms of combating money laundering and terrorist financing.

5 *Suspicious Transaction Report*.

6 *Suspicious Activity Report*.

Threat level substantiation	Financing of terrorism through opened bank accounts, both company accounts as well as private accounts, is one of the simplest methods to use. The accounts may be supplied both with legal resources as well as with assets from illegal sources. This mode is broadly available due to the well-developed banking system, and it costs little to use it. Making transactions on bank accounts does not require specialised knowledge or skills. The use of the banking system, primarily bank accounts, due to the possibility of making quick deposit and payment transactions through them, is easy, and does not require complex planning. If a terrorist organisation creates a system of fictitious entities having bank accounts in the country and abroad, it can make transfers and payments between these entities, which, from the point of view of substantiated economic interest, will not be suspicious and will be very hard to question. It is relatively easy to hide the true purpose of resources in a high volume of legal transactions, in particular in case of transactions of relatively low value. The GIFI has information that this *modus operandi* can be used for financing of terrorism. CONCLUSION: The use of a bank account to collect and transfer money for the benefit of terrorists constitutes a very high risk of financing of terrorism.

Table no. 2

Type of services, financial products used	credits and loans
General risk description	acquiring loans or credits from financial institutions without the will to repay the emerging obligations
Risk emergence scenario (e. g. possible example of the emergence of risk)	Acquiring short- or long-term loans by natural persons that permit financial support for terrorists, in particular to travel to conflict zones in order to fight in the ranks of foreign terrorist fighters.
Vulnerability level	2
Vulnerability level substantiation	Access to credits and loans provided by banks is simple, however, certain limitations exist that are mainly related to the customer having suitable credit ability and suitable security. For these reasons, the possibility to use straw men or shell companies to acquire credits and loans is more limited. The repayment of credits and loans may also take place by way of international transactions, including through the usage of third persons or parties. Pursuant to information from the website of the Polish Credit Information Office (BIK) in the year 2018 an increase was noted in terms of the provided loans, both in terms of their count as well as value. In the year 2018, banks and cooperative savings and loan unions provided a total of 7.5 m consumer loans, meaning, 2.8% more than in 2017 (in terms of value – the increase was 6.7% as compared to the

	preceding year).[7] An increase was also noted of the count and value of awarded mortgage loans (by 10.3% and 20.1% more than in the year 2017, respectively). A slight drop was seen solely in the number of credit cards given out (by ca. 0.6% compared to 2017), however the value of their limits was higher by ca. 2.2% than the value of credit card limits in the year 2017.[8] All entities offering the above-described products/services are OI. These entities apply customer due diligence measures, even though audits continue to reveal shortcomings in this area. They are aware of their obligations in terms of AML/CTF.[9] They analyse transactions efficiently – the majority of STR/SAR, transferred to the GIFI, originate from banks/branches of credit institutions/branches of foreign banks (in the year 2017 this was ca. 94.9% SARs from OI and ca. 97.8% STRs). Public administration authorities have knowledge on ML/TF risk in this regard. The GIFI is able to collect and analyse information. There exists the probability that a case of TF is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of domestic and international cooperation of public administration bodies is relatively good. Existing legal provisions correspond mostly to the scope of the analysed risk.
Threat level	3
Threat level substantiation	Taking out loans or credits with financial institutions without the will to repay the financial obligations entered into can be seen in Poland as quite an attractive method of financing of crime in the form of terrorism. This applies in particular to private credits and loans, and to a much more limited extent – mortgage loans. Simplified procedures used to obtain such credits or loans and the large variety of banks or companies offering loans influences the attractiveness of such a *modus operandi*. This does not require specialised knowledge, planning or unique skills from members of a terrorist organisation or their supporters. In certain cases, however, counterfeiting of documents may be necessary. Information on the use of this *modus operandi* for financing of terrorism stems mainly from abroad. CONCLUSION: Taking out loans or credits with financial institutions without the will to repay the emerging obligations constitutes a high risk of financing of terrorism.

Table no. 3

[7] https://media.bik.pl/informacje-prasowe/420017/perspektywy-rynku-kredytowo-pozyczkowego-na-rok-2019, access on 14.06.2019.

[8] https://media.bik.pl/publikacje/read/420072/newsletter-kredytowy-bik-grudzien-2018-r-i-podsumowanie-roku-kredytowe, access on 14.06.2019.

[9] However, all audits carried out in the year 2018 by the Polish Financial Supervision Authority (e. g. at 12 commercial banks and three cooperative banks) revealed irregularities and divergences in the analysed areas (mainly spanning risk assessment and application of customer due diligence measures, as well as the organisation of the process of countering money laundering and financing of terrorism and the transfer of information to the GIFI). The GIFI in turn during four out of five bank audits conducted in the years 2017-2018 revealed irregularities in the execution of obligations in terms of combating money laundering and financing of terrorism

Type of services, financial products used	anonymous prepaid cards – electronic money carriers released by foreign entities – electronic money institutions offering their Products in Poland using the European passport
General risk description	usage of anonymous prepaid cards to hinder the identification of persons making transactions related to the financing of terrorism
Risk emergence scenario (e. g. possible example of the emergence of risk)	1. Resources foreseen for financing of terrorism are transferred between natural persons with the use of prepaid cards ensuring anonymity both of the card purchaser as well as the beneficiaries of the resources collected on it. 2. Sponsoring terrorist activity by way of purchasing anonymous prepaid cards that can be used internationally (including international calling cards or cards for on-line games) and transferring the card numbers to persons related to terrorists. The card (or, precisely, their descriptions and numbers) are sold by the above described persons, with the acquired resources being used to finance criminal activity. 3. The resources that top up anonymous prepaid cards and which are provided by various persons, are transferred to various bank accounts held or controlled by terrorists or paid out in cash. 4. The use of electronic cash portfolios by terrorists to collect cash assets under various titles, including for charity persons, and then transferring the resources to payment cards (including anonymous prepaid cards), the money from which is withdrawn in cash.
Vulnerability level	2
Vulnerability level substantiation	Access to prepaid cards being carriers of electronic money is relatively easy (via the Internet). The main source of risk of financing of terrorism are anonymous prepaid cards offered in Poland, but issued by issuers from other EU countries. There exists the possibility of issuing electronic money lawfully (stored on the prepaid card or a server), with the identification and verification of customers, however in this regard there are limits to amounts stored on the payment instruments as well as limits of transaction amounts as set out in directive 2018/843[10]. Electronic money and prepaid cards can be used to conduct international transactions. Due to the execution of oversight over foreign electronic money institutions offering their products and services in Poland by the authorities of the EU member country of origin, it should be assumed that these have and adhere to procedures in terms of anti-money laundering and countering financing of terrorism (it is worth remembering, however that these are not OI as understood by Polish provisions, as long as they do not operate via branch offices set up in Poland). Public administration authorities have knowledge on ML/TF risk in this regard. The GIFI is able to collect[11] and analyse information, they are, however, largely dependent in this regard on information obtained from foreign Financial Intelligence Units. There exists the possibility that a case of TF is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of domestic and international cooperation of public administration bodies is relatively good. Existing legal provisions mostly correspond to the scope of the analysed risk.
Threat level	1

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

[11] Pursuant to art. 53 section 1 of directive no. 2015/849, if a given financial intelligence unit receives a report on a suspect transaction that applies to another EU member state (e. g. Poland), it immediately transfers it to a FIU from that member state.

Threat level substantiation	Domestic banks only issue prepaid cards being a type of debit card. Anonymous prepaid cards – carriers of electronic money – are issued by electronic money institutions from other EU member states and offered to customers in Poland. It should be assumed that the risk of financing of terrorism could apply primarily to these cards purchased by natural persons. This requires perpetrators to know the offers of foreign electronic money institutions. There is information, mainly from abroad, about the use of this *modus operandi* for FT. CONCLUSION: The usage of anonymous prepaid cards to hinder the identification of persons making transactions related to the financing of terrorism currently has a low level of threat in Poland.

Table no. 4

Type of services, financial products used	transfers of funds
General risk description	usage of transfers to move funds to other jurisdictions
Risk emergence scenario (e. g. possible example of the emergence of risk)	1. The use of transfers of funds to move resources under fictitious titles (e. g. for the purpose of helping the family). The resources are transferred to banks located in countries bordering on the places of activity of terrorist organisations. 2. A bank employee cooperating with the perpetrators accepts from them the funds stemming from illegal sources, which are then transferred by way of cashless transactions to bank accounts indicated by them, hiding their source and purpose
Vulnerability level	2
Vulnerability level substantiation	Ordering of transfers of funds via banks is relatively easy. Some banks also provide services entailing the transfer of funds in name of foreign payment institutions. There exists a limited volume of products simplifying anonymous transactions (this may be possible when making occasional transactions below the threshold equal to 1,000 Euro or in case of using a straw man or shell company). Movements of funds are often international in character. According to the study of the NBP entitled *Comparison of selected components of the Polish payment system with the systems of other EU countries for the year 2017*, the total number of transfers amounted to ca. 2.62 billion in the year 2017.[12] In terms of the number of per capita transfer orders, Poland ranks above the EU average. All entities offering the above-described products/services are OI. These entities apply customer due diligence measures, even though audits continue to reveal shortcomings in this area. They are aware of their obligations in terms of AML/CTF.[13] They analyse transactions efficiently – the majority of STR/SAR, transferred to the GIFI, originate from banks/branches of credit institutions/branches of foreign banks (in the year 2017 these were ca. 94.9% SARs from OI and ca. 97.8% STRs). Public administration authorities have knowledge on ML/TF risk in this regard. The GIFI is able to collect and analyse information. The probability is high that a case of FT is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of domestic and international cooperation of public administration bodies is relatively good.

[12] Comparison of selected components of the Polish payment system with the systems of other EU countries for the year 2017, NBP, December 2018, p. 32, at: https://www.nbp.pl/home.aspx?f=/systemplatniczy/obrot_bezgotowkowy/obrot_bezgotowkowy.html.

[13] However, all audits carried out in the year 2018 by the Polish Financial Supervision Authority (e. g. at 12 commercial banks and three cooperative banks) revealed irregularities and divergences in the analysed areas (mainly spanning risk assessment and

Threat level	3
Threat level substantiation	Financing of terrorism through the use of transfers to move financial resources to other jurisdictions is one of the most commonly encountered methods. This mode is widely available due to the well-developed world banking system, and it costs relatively little to make use of it. Ordering transfers does not require knowledge about the banking system or special skills, however, the implementation of this *modus operandi* is relatively safe then, if the bank, due to the character of the transaction or the place of the transaction, is not obligated to apply enhanced customer due diligence measures. These hazards could be circumvented by e. g. recruitment of a bank employee for cooperation. If a terrorist organisation would create a system of shell companies holding bank accounts domestically and abroad, it could make transfers between entities, which transactions, from the point of view of financial substantiation, would not be suspicious and would be very difficult to question. The use of transfers to move financial resources to other jurisdictions in the banking system is easy, does not require complex planning, specialised knowledge or skills. CONCLUSION: The use of transfers to move financial resources to other jurisdictions for purposes of terrorist activity creates a very high threat of financing of terrorism.

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

Table no. 5

Type of services, financial products used	money transfers
General risk description	usage of providers of financial resource transfer services to move funds foreseen for financing of terrorism
Risk emergence scenario (e. g. possible example of the emergence of risk)	1. Usage by persons related to terrorists of the possibility of applying by financial asset transfer service providers of simplified customer due diligence measures for low transaction amounts. This allows for the transfer of resources in a manner hindering the identification of the originator and the beneficiary. The deposit of financial resources takes place in Poland, and the withdrawal in countries characterised by high activity of terrorist organisations. 2. Usage of money transfers to financially support foreign terrorist fighters remaining in or travelling to conflict zones. 3. Usage by persons financing terrorism of the services of providers that are active in Poland, who however do not transfer information about suspicious transactions to Polish Financial Intelligence Unit.
Vulnerability level	2

application of customer due diligence measures, as well as the organisation of the process of countering money laundering and financing of terrorism and the transfer of information to the GIFI). The GIFI in turn during four out of five bank audits conducted in the years 2017-2018 revealed irregularities in the execution of obligations in terms of combating money laundering and financing of terrorism.

Vulnerability level substantiation	Cash transfer services are relatively easily available. There exists a limited possibility to hide identification data of principals and beneficiaries of fund transfers in case of making sporadic transactions below the threshold corresponding to 1,000 Euro or in case of usage of a mule or a simulating company. Fund transfers are frequently international in character. Almost all entities offering such services are OI save for payment institutions from other EU member states providing payment services in Poland via agents . These entities have a certain level of awareness of their duties in the area of AML/CTF, even though shortcomings continue to be revealed in terms of their execution.[14] They provide relatively few SARs and STRs (in the year 2017 – 0.58% of all SARs received from OI and 0.034% of all received STRs). Public administration authorities have knowledge on ML/TF risk in this regard. The GIFI is able to collect and analyse information. There exists the probability that a case of TF is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of domestic and international cooperation of public administration bodies is relatively good. Existing legal provisions correspond mostly to the scope of the analysed risk.
Threat level	3
Threat level substantiation	For low-amount transactions, the providers of financial asset transfer services may apply simplified customer due diligence measures. Resources may be transferred that stem from entirely legal sources. Presently, terrorist activity is a low-cost activity (for instance, the cost of a terrorist attack at a bus stop in Israel is ca. 200 USD, and the cost of the 2004 Madrid bombing did not exceed 10 000 USD). It appears ever more frequently in the form of self-financing of terrorists. It is one of the most frequently used, known methods of financing to receive a single or several low-amount money transfers. It is a broadly available mode, its application costs little, and is perceived by perpetrators to be attractive. The payer does not need an account to execute this kind of money transfer. To hide the actual beneficiary, straw men or family are frequently used. The usage of financial asset transfer service providers to transfer money from legal or illegal sources requires minimal specialised knowledge about the resource transfer system, it is relatively inexpensive in terms of fees, and relatively safe. CONCLUSION: The above information and the fact that persons from elevated risk states and regions remain in Poland cause the usage of the method with service providers in the area of financial asset transfers to transfer money – as cash transfers – foreseen for financing of terrorism, to be a high-level threat of financing of terrorism.

Table no. 6

Type of services, financial products used	on-line payment services
General risk description	usage of on-line payment services by entities participating in the process of financing of terrorism, in particular by potential foreign terrorist fighters

[14] During all audits conducted in the year 2018 by the Polish Financial Supervision Authority (e. g. at 16 domestic payment institutions), irregularities and discrepancies were disclosed in the analysed areas (mainly in terms of risk assessment and the application of customer due diligence measures, as well as the organisation of the process of countering money laundering as well as financing of terrorism and transferring information to the GIFI). However, the GIFI revealed during all three audits of payment institutions conducted in the years 2017-2018, discrepancies in the fulfilment of obligations concerning combating money laundering and financing of terrorism.

Risk emergence scenario (e. g. possible example of the emergence of risk)	1. Usage of on-line payment services by foreign terrorist fighters to make purchases at on-line stores of equipment necessary to remain in conflict zones. 2. Usage of the discussed services by persons depositing money for charity organisations that participate in the process of financing of terrorism. 3. Moving funds between the individual persons engaged in terrorist activity. 4. Usage of cashless money transfers (below the threshold requiring customer identification) to transfer funds under fictitious purposes (e. g. as aid for the family). The resources are transferred to agencies of payment institutions located in countries bordering the location of activity of terrorist organisations. 5. An agent (or employee) of a payment institution, cooperating with terrorists, accepts from them or their supporters financial resources, which are then transferred via cashless transfers to bank accounts indicated by them, hiding their source and purpose.
Vulnerability level	3
Vulnerability level substantiation	On-line transfer services are relatively easily available – all it takes is to have Internet access. There exist possibilities to hide identification data of the person using these types of payment services (e. g. one website provides the possibility of making transactions up to a specific amount without the verification of identification data, with the verification of identification data being simplified – it is based on a scan of a passport or driver's licence, webcam photograph and geolocation data of the customer as conveyed by them). Transfers of funds are frequently international in character. Only a part of entities offering these services are OI. Payment institutions providing payment services by on-line platforms, registered in other countries, are not OI. OI from the area of payment services have a certain awareness of their duties in terms of AML/CTF, even though shortcomings continue to be revealed in terms of their execution.[15] They provide relatively few SARs and STRs (in the year 2017 – 0.58% of all SARs received from OI and 0.034% of all received STRs). Public administration authorities have knowledge on ML/TF risk in this regard. The GIFI is able to collect and analyse information. There exists the probability that a case of TF is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of domestic and international cooperation of public administration bodies is relatively good. Existing legal provisions mostly correspond to the scope of the analysed risk.
Threat level	3

[15] During all audits conducted in the year 2018 by the Polish Financial Supervision Authority (e. g. at 16 domestic payment institutions), irregularities and discrepancies were disclosed in the analysed areas (mainly in terms of risk assessment and the application of customer due diligence measures, as well as the organisation of the process of countering money laundering as well as financing of terrorism and transferring information to the GIFI). However, the GIFI revealed during all three audits of payment institutions conducted in the years 2017-2018, discrepancies in the fulfilment of obligations concerning combating money laundering and financing of terrorism.

Threat level substantiation	The usage of Internet-based payment services that provide *online* payments and fund transfer over the Internet, being an electronic alternative to traditional methods such as cheques and payment orders, is a relatively attractive method of financing of terrorism. Terrorist undertakings belong among relatively cheap investments as compared to the losses they cause and the panic that is caused. Presently, persons remain in Poland from elevated-risk states and regions, for whom the offered payment services allowing entrepreneurs and consumers using *e-mail* addresses to send and receive payments on-line are attractive. Due to the transfers concerning relatively low amounts, the cash flows may not necessarily be recognised as suspicious, and are furthermore simple to use, even if they require planning and knowledge. CONCLUSION: The use of on-line payment services creates a high threat of financing of terrorism.

Table no. 7

Type of services, financial products used	Hawala-type transfer systems
General risk description	usage of Hawala networks or other informal asset transfer systems for financing of terrorism
Risk emergence scenario (e. g. possible example of the emergence of risk)	1. Depositing of cash assets in the state of X, characterised by a high level of terrorist threat, coupled with a withdrawal in Poland to finance terrorist activity. Usage of an informal criminal network of resource transfer to prevent the possibility of disclosure of funds. 2. Resources provided for the purpose of financing of terrorism are mixed with other cash transfers within the Hawala network to hide the trace of the transactions being conducted. 3. Usage of entities offering illegal payment services to transfer money for the benefit of terrorists. For instance, a person offering such services uses bank accounts to which they deposit cash assets from their customers. The assets are then transferred to the accounts of entities offering legal payment services. As part of these services, for instance, gold is used to clear transactions. It is easy to liquidate, in particular in certain Asian and African countries, where extensive markets trading in this metal exist.
Vulnerability level	4
Vulnerability level substantiation	Services of Hawala systems greatly simplify making quick and anonymous transactions. Due to the fact that they are provided by entities remaining outside of state control – there is no data concerning the volume and value of transactions executed as part of this system in Poland. Entities offering these services are not OI. Public administration authorities have knowledge on ML/TF risk in this regard. The GIFI has no possibility of collecting and analysing information from these kinds of entities. There exists the possibility that a case of TF within the scope of the analysed risk is not detected. The level of domestic and international cooperation of public administration bodies is relatively good. Existing legal provisions mostly correspond to the scope of the analysed risk.
Threat level	2

Threat level substantiation	A Hawala-type system is a kind of informal banking system. It is used, among others, in international trade, often to move money over long distances. A significant component of it is the possibility of maintaining full anonymity and utilising several intermediaries when ordering the transfer. The person withdrawing the cash is not asked to show any identification and is usually unknown or weakly known to the relevant broker. It is similar for the withdrawing party, who may pick up the transferred funds by only providing a specified password. In this way, the entity offering services in a Hawala system usually does not know, from whom, what for and for whom the transaction is being done. The key factor is the trust between the intermediaries, who usually belong to a single family, a circle of friends or recommended parties and operate in a few or several countries. It is also important that the paying and withdrawing parties do not need to have any bank accounts in those countries (frequently, due to restrictive local banking laws, they are unable to open such an account in that country). The size (volume) of payments/transactions executed through such informal systems is not known. There are no numerous ethnic minorities in Poland, in which Hawala-type systems would be commonplace (however, a rising number of foreigners from elevated-risk countries, remaining in Poland, was noticed). Polish services have noted cases of usage of this method to move funds foreseen for terrorist activity. CONCLUSION: The threat level from the use of the informal Hawala banking system to transfer funds for purposes of financing of terrorist activity creates a medium-level threat of financing of terrorism.

3. Area - insurance

Table no. 8

Type of services, financial products used	motor vehicle insurance
General risk description	using deception to obtain damage compensation from insurance to finance terrorism
Risk emergence scenario (e. g. possible example of the emergence of risk)	Purposeful traffic accidents in order to obtain damage compensation that will be used for the financing of terrorism.
Vulnerability level	4
Vulnerability level substantiation	It is relatively easy to acquire motor vehicle insurance. The identification data of the insured or endowed person is difficult to hide. It is possible to conduct an international transaction of the customer of a Polish insurance company is a resident of a different country or if they are making the financial transaction via a foreign account. Entities offering such services are not OI. Public administration authorities have knowledge on ML/TF risk in this regard. The GIFI is unable to collect and analyse information on such services. There exists the probability that a case of TF spanning the analysed scenarios is not detected. The level of domestic and international cooperation of public administration bodies is relatively good. Existing legal provisions largely do not correspond to the scope of the analysed risk.
Threat level	1

Threat level substantiation	The usage of the mechanism of fraudulently seeking compensation for damage from insurance may be a form of financing of terrorism. However, the level of complexity of the procedure to acquire the damage compensation, prepare the necessary documentation, and the risk of contact with law enforcement authorities cause this form of financing of terrorist activity to be unattractive. In Poland, there is no clear information about the use of this *modus operandi* for financing of terrorism. It is difficult to use due to the need to have specialised knowledge, and there exist cheaper and simpler ways to finance terrorist activity. CONCLUSION: The usage of the method of fraudulent acquisition of resources from insurance to gather funds for financing terrorist activity constitutes a low threat level of financing of terrorism.

Table no. 9

Type of services, financial products used	life insurance
General risk description	use of capacities offered by life insurance for financing of terrorism
Risk emergence scenario (e. g. possible example of the emergence of risk)	The cancellation of a life insurance policy to acquire resources from the premiums paid beforehand before foreign terrorist fighters travel to conflict zones.
Vulnerability level	1
Vulnerability level substantiation	It is relatively easy to acquire life insurance/endowment. The identification data of the insured or endowed person is difficult to hide. It is possible to conduct an international transaction in case when the customer of a Polish insurance company is a resident of a different country or if he/she makes the financial transaction via a foreign account. All entities offering such services are OI. They are aware of their obligations in terms of AML/CTF, even though relatively little information about suspicious transactions/activity is provided by life insurance companies (in the year 2017 it was 0.12% of all SARs from OI and 0.16% of all STRs). Public administration authorities have knowledge on ML/TF risk in this regard. The GIFI is able to collect and analyse information. There exists the probability that a case of TF is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of domestic and international cooperation of public administration bodies is relatively good. Existing legal provisions correspond to the scope of the analysed risk.
Threat level	1
Threat level substantiation	The usage of financial resources stemming from a cancelled life insurance policy can be a form of financing of terrorism. However, this m*odus operandi* can be relatively expensive due to the fact of possibility of loss of a portion of the funds (related to conditions of the insurance contract), and due to this the level of attractiveness of this form of financing terrorism is relatively low. In Poland, with no cases of travel of terrorist fighters to conflict zones being noted, there is no clear information about the usage of this *modus operandi* for financing of terrorism. There exist cheaper and simpler ways to finance terrorist activity. CONCLUSION: The usage of financial resources from a cancelled life insurance policy to finance terrorist activity, in particular travel by fighters to conflict zones, constitutes a low-level threat of financing of terrorism.

4. Area – other financial institutions

Table no. 10

Type of services, financial products used	services on the FOREX currency market
General risk description	usage of a broker company operating on the FOREX market to commit fraud to obtain resources for financing of terrorism

Risk emergence scenario (e. g. possible example of the emergence of risk)	1. Perpetrators register a company that starts operations as a FOREX market broker without acquiring the relevant licence to conduct investment/broker services. The offer of the company is available in several languages, and encourages through high profits. Thanks to this, and thanks to the use of aggressive marketing techniques, a customer base is established who make payments to accounts of the entity, to credit their broker accounts. Investors are not aware that the transactions they are making are fictitious, and that the resources at one point will be taken over by the illegally operating investment company. In case of companies that are so-called *market makers*[16], it is conceivable that they will be offered worse conditions than the market offers so that they suffer losses, with resources obtained in this way being provided to terrorist organisations. 2. Perpetrators register a company that starts operations as a FOREX market broker without acquiring the relevant licence to conduct investment/broker services. Supporters of terrorist organisations who transferred resources conduct transactions that are unfavourable to them (especially if the company operates as a *market maker*) or consent to elevated commission or the loss of funds when the entity ceases operations. The resources obtained in this way are transferred to terrorist organisations.
Vulnerability level	2
Vulnerability level substantiation	Services on the FOREX market are available via brokers. It is rather difficult to hide the identification data of the party ordering transactions on this market by a licensed broker. International transactions may be the case if the customer is a resident of a different country or conducts a financial transaction via a foreign account, or uses the services of a foreign entity. All entities offering such services are OI (brokerage houses or banks that include brokerage agencies in their structures) – however customers may make use of services offered on-line by foreign entities. OI in this area have a certain awareness of their duties in terms of AML/CTF, even though shortcomings continue to be revealed in terms of their execution.[17] Relatively little information about suspicious transactions/activity is transferred by brokerage houses (in the year 2017 it was 0.49% of all SARs from OI and 0.42% of all STRs). Public administration authorities have knowledge on ML/TF risk in this regard. The GIFI is able to collect and analyse information. The probability is high that a case of TF is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of domestic and international cooperation of public administration bodies is relatively good. Existing legal provisions mostly correspond to the scope of the analysed risk.
Threat level	1
Threat level substantiation	FOREX is an international wholesale currency exchange market, as part of which banks, large international corporations and institutional investors from all over the world conduct currency exchange operations around the clock using phone lines, computer connections and IT systems. The utilisation of a legal company – albeit one without a suitable licence to conduct investment/broker activity and controlled by criminals – operating on the FOREX market as a broker in the *market maker* model is a method of acquisition and transferring funds for terrorist activity that has low attractiveness. This *modus operandi* requires specialised knowledge about the currency exchange market, skills as well as planning. In the *market maker* model, the losses from

[16] An entity issuing and quoting financial instruments acts at the same time as the other party in transactions concluded by the customer.

[17] During all audits conducted in the year 2018 by the Polish Financial Supervision Authority (e. g. at six brokerage houses/ agencies), irregularities and discrepancies were disclosed in the analysed areas (mainly in terms of risk assessment and the application of customer due diligence measures, as well as the organisation of the process of countering money laundering as well as financing of terrorism and transferring information to the GIFI). The GIFI revealed in turn, during a single audit of a brokerage house conducted in the year 2017, discrepancies in the fulfilment of obligations concerning combating money laundering and financing of terrorism.

	participation in the FOREX market used by investors (due to fraud or conscious activity) are the profit of the broker and may be transferred to terrorist organisations. GIFI has no information on the scope of use of this *modus operandi*. CONCLUSION: The usage of a broker company operating on the FOREX market as a *market maker* to commit fraud to obtain resources for terrorist activity constitutes a low level of threat of financing of terrorism.

Table no. 11

Type of services, financial products used	investment fund (IF) share units
General risk description	trade in investment fund share units in order to collect funds for terrorist activity
Risk emergence scenario (e. g. possible example of the emergence of risk)	Perpetrators regularly buy share units in investment funds for minor amounts to subsequently sell them after accumulation, and transfer the resources abroad.
Vulnerability level	2
Vulnerability level substantiation	Access to investment fund (IF) share units is relatively easy. It is difficult to hide the identification data of investment fund customers. International transactions may emerge in relation to the purchase and sale of share units only if the customer of a Polish IF would be a resident of a different country, or if they would be making a financial transaction via a foreign account, or if the share units are being bought from a foreign IF. All entities offering such services are OI – however customers may make use of services offered by foreign entities. OI in this area have a certain awareness of their duties in terms of AML/CTF, even though shortcomings continue to be revealed in terms of their execution.[18] Relatively little information about suspicious transactions/activity is transferred by TFI/IF (in the year 2017 it was 0% of all SARs from OI and 0.09% of all STRs). Public administration authorities have knowledge on ML/TF risk in this regard. The GIFI is able to collect and analyse information. The probability is high that a case of TF is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of domestic and international cooperation of public administration bodies is relatively good. Existing legal provisions mostly correspond to the scope of the analysed risk.
Threat level	1
Threat level substantiation	The purchase of and trade in investment fund share units to collect funds for terrorist activity can be a *modus operandi* for financing of terrorism. However, the GIFI had no information on the investment of illegal or legal assets in investment funds for this purpose. Trade in investment fund share units is a form of activity that is difficult to apply due to the necessity of having specialised knowledge about the capital market, and cheaper and simpler ways of financing terrorist activity exist. CONCLUSION: The usage of purchase of and trade in investment fund share units to collect funds for terrorist activity constitutes a low threat of financing of terrorism.

Table no. 12

Type of services, financial products used	security accounts and cash accounts used to handle them
General risk description	the usage of security accounts and cash accounts used to handle them to collect funds for terrorist activity

[18] During all audits of investment fund associations executed by the GIFI in the years 2017, discrepancies were revealed in the fulfilment of obligations concerning combating money laundering and financing of terrorism.

Risk emergence scenario (e. g. possible example of the emergence of risk)	1. Using companies established in particular in tax havens, the perpetrators deposit resources acquired from illegal or legal sources on the capital market. The purchased securities are then sold, and the obtained funds are used to finance terrorist activity. 2. Resources are moved from a bank account held in a different country to an account used to service a securities account belonging to a foreign company controlled by supporters of a terrorist organisation, for the benefit of a natural person under a fictitious reference of investment in shares in a public company. The resources are then – within a short amount of time – transferred to a bank account held in a third country, belonging to the above company, as profit from trade in securities.
Vulnerability level	2
Vulnerability level substantiation	It is relatively easy to open these types of accounts. It is rather difficult to hide customer identification data. There are international transactions. All entities offering such services are OI. They have a certain awareness of their obligations in terms of AML/CTF, even though shortcomings continue to be revealed in terms of their execution.[19] Relatively little information about suspicious transactions/activity is transferred by brokerage houses (in the year 2017 it was 0.49% of all SARs from OI, and 0.42% of all STRs). Public administration authorities have knowledge on ML/TF risk in this regard. The GIFI is able to collect and analyse information. The probability is high that a case of TF is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of domestic and international cooperation of public administration bodies is relatively good. Existing legal provisions mostly correspond to the scope of the analysed risk.
Threat level	1
Threat level substantiation	The usage of securities accounts and cash accounts used to handle them to collect funds for terrorist activity can be a form of financing of terrorism. However, the level of complexity of the securities market makes this method of financing of terrorist activity unattractive. There is no clear information on the use of this *modus operandi* for financing of terrorism. It is difficult to apply due to the necessity of having specialised knowledge of the capital market, and cheaper and simpler ways of financing terrorist activity exist. CONCLUSION: The usage of securities accounts and cash accounts used to handle them to collect funds for terrorist activity constitutes a low threat of financing of terrorism.

5. Area – currency exchange

Table no. 13

Type of services, financial products used	cash-based foreign currency exchange
General risk description	foreign currency exchange to hinder identification of the crime of financing of terrorism
Risk emergence scenario (e. g. possible example of the emergence of risk)	1. Use by persons related to terrorist organisations of currency exchange at exchange offices to make it more difficult for law enforcement authorities to retrace the path of transfer of assets. Usage of "trusted" exchange offices that do not report suspicious transactions to relevant financial intelligence units.

[19] During all audits conducted in the year 2018 by the Polish Financial Supervision Authority (e. g. at six brokerage houses/ agencies), irregularities and discrepancies were disclosed in the analysed areas (mainly in terms of risk assessment and the application of customer due diligence measures, as well as the organisation of the process of countering money laundering as well as financing of terrorism and transferring information to the GIFI). The GIFI revealed in turn, during a single audit of a brokerage house conducted in the year 2017, discrepancies in the fulfilment of obligations concerning combating money laundering and financing of terrorism.

	2. Exchanging the collected money (e. g. collected from supporters) for high-denomination notes in other currencies (commonly traded all over the world, e. g. EUR) at exchange offices, to make them easier to transport across state borders.
Vulnerability level	2
Vulnerability level substantiation	Access to currency exchange is very easy. It is easy to hide the identification data of the person making the transaction, in particular if the individual transactions are made at relatively small amounts. It is possible to execute international transactions if at least a part of these is made in cashless form. All entities offering such services are OI. They are aware of their obligations in terms of AML/CTF.[20] Relatively little information about suspicious transactions/activity is transferred by entities dealing in foreign currency exchange[21] (in the year 2017 these were ca. 0.03% of all SARs from OI and ca. 0.0064% of all STRs, meaning a drop as compared to data for the year 2016, when these were ca. 0.64% of all SARs and ca. 7.66% of all STRs). Public administration authorities have knowledge on ML/TF risk in this regard. The GIFI is able to collect and analyse information. The probability is high that a case of TF is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of domestic and international cooperation of public administration bodies is relatively good. Existing legal provisions correspond to the scope of the analysed risk.
Threat level	2
Threat level substantiation	The usage of the foreign currency exchange mechanism to hinder identification of the crime of financing of terrorism is a method that is relatively easy to use and broadly available. It costs little to make use of it, and it is perceived by perpetrators to be rather attractive, in particular as funds may stem from entirely legal sources. Foreign currency exchange transactions below the threshold of registration usually do not raise suspicions. The high exchange office turnover volume permits the hiding of illegal or legal funds among entirely legal singular transactions. The GIFI has received very limited information about this method being used for financing of terrorist activity. CONCLUSION: Usage of the currency exchange mechanism to hinder the identification of the crime of financing of terrorism constitutes a medium-level threat of financing terrorism.

Table no. 14

Type of services, financial products used	money exchange within a single currency
General risk description	exchange of low-value banknotes against higher-value banknotes.
Risk emergence scenario (e. g. possible example of the emergence of risk)	Exchanging low-value EUR banknotes against 500 EUR banknotes in order to reduce the volume of the cash resources carried.
Vulnerability level	2

[20] An audit conducted by the NBP showed that the share of entrepreneurs operating exchange offices, where discrepancies were disclosed spanning the execution of obligations concerning AML/CTF as compared to all audited entrepreneurs operating exchange offices were small, amounting to 4.87% in the year 2018, and 4.14% in the year 2017. However, in case of all three audits conducted by the GIFI in the year 2017 at OI dealing in currency exchange, certain irregularities were discovered.

[21] With the exclusion of services rendered by banks.

Vulnerability level substantiation	Access to currency exchange is very easy. It is easy to hide the identification data of the person making the transaction, in particular if the individual transactions are made at relatively small amounts. It is possible to execute international transactions if at least a part of these is made in cashless form. All entities offering such services are OI. They are aware of their obligations in terms of AML/CTF.[22] Relatively little information about suspicious transactions/activity is transferred by entities dealing in foreign currency exchange[23] (in the year 2017 these were ca. 0.03% of all SARs from OI and ca. 0.0064% of all STRs, meaning a drop as compared to data for the year 2016, when these were ca. 0.64% of all SARs and ca. 7.66% of all STRs). Public administration authorities have knowledge on ML/TF risk in this regard. The GIFI is able to collect and analyse information. The probability is high that a case of TF is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of domestic and international cooperation of public administration bodies is relatively good. Existing legal provisions correspond to the scope of the analysed risk.
Threat level	2
Threat level substantiation	The usage of the mechanism of exchanging low-denomination banknotes against higher-denomination banknotes for the purpose of financing of terrorism is a broadly available mode, and it costs little to use it. It may be perceived by perpetrators as attractive. Physical carriage of banknotes foreseen for financing of terrorism should not attract attention, and the reduction of the volume of the cash being transported reduces the risk of it being discovered or accidentally lost. However, the safety of this method requires planning, adherence to the rule of making low-quantity operations. The exchange of wrinkled, frequently dirty banknotes of low denominations can cause attention. This method most commonly requires the cooperation of persons employed at institutions such as a bank or an exchange office. The GIFI received very limited information on the possibility of using this method for financing of terrorist activity. CONCLUSION: The usage of the mechanism of exchanging low-denomination cash against higher-denomination banknotes constitutes an average risk of financing of terrorism.

Table no. 15

Type of services, financial products used	services of entities offering cashless foreign currency exchange
General risk description	cashless currency exchange related to fund transfers
Risk emergence scenario (e. g. possible example of the emergence of risk)	Usage by persons related to terrorist organisations cashless currency exchange at so-called on-line exchange offices to make it more difficult for law enforcement authorities to retrace the asset transfer path. For instance – funds in PLN are transferred to a so-called on-line exchange office from a bank account with a certain institution with the order to exchange them against USD and transfer to an account at a different bank, belonging in reality to a different entity than the original originator.
Vulnerability level	2

[22] An audit conducted by the NBP showed that the share of entrepreneurs operating exchange offices, where discrepancies were disclosed spanning the execution of obligations concerning AML/CTF as compared to all audited entrepreneurs operating exchange offices were small, amounting to 4.87% in the year 2018, and 4.14% in the year 2017. However, in case of all three audits conducted by the GIFI in the year 2017 at OI dealing in currency exchange, certain irregularities were discovered.

[23] With the exclusion of services rendered by banks.

Vulnerability level substantiation	Access to currency exchange services is very easy. It is easy to hide the identification data of the person making the transaction, in particular if the individual transactions are made in relatively small amounts. It is possible to execute international transactions if these transactions are made in cashless form. All entities offering such services are OI. They have a certain awareness of their obligations in terms of AML/CTF.[24] Relatively little information about suspicious transactions/activity is transferred by entities dealing in foreign currency exchange[25] (in the year 2017 these were ca. 0.03% of all SARs from OI and ca. 0.0064% of all STRs, meaning a drop as compared to data for the year 2016, when these were ca. 0.64% of all SARs and ca. 7.66% of all STRs). Public administration authorities have knowledge on ML/TF risk in this regard. The GIFI is able to collect and analyse information. There exists the probability that a case of TF is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigations. The level of domestic and international cooperation of public administration bodies is relatively good. Existing legal provisions partly correspond to the scope of the analysed risk.[26]
Threat level	2
Threat level substantiation	The usage of the mechanism of cashless foreign currency exchange at so-called on-line exchange offices together with the transfer of funds to make it more difficult for law enforcement authorities to trace the path of asset values is an identified method allowing financing of terrorism. Presently, on-line exchange offices are not legally licensed. They are not the subject of any act of law or any single authority that would control the scope of their activity. According to estimates available on-line, in the first six months of 2017 ca. 35% of foreign currency exchange transactions took place on-line.[27] The volume of turnover of on-line exchange offices is rising dynamically, and individual transactions can even amount to a few million PLN. The cashless currency exchange connected to the transfer of funds is fairly cheap and as a *modus operandi* can be perceived by perpetrators as an attractive and broadly accessible method of financing of terrorism. Under conditions of dynamic economic growth by businesses dealing in export or import, cashless exchange transactions at on-line exchange offices may be relatively invisible for the supervision (in particular in case of the lack of clear legal provisions). The GIFI had received very limited information on the possibility of usage of this method for financing of terrorist activity. CONCLUSION: The usage of the mechanism of cashless currency exchange at so-called on-line exchange offices together with the transfer of funds creates a medium-level threat of financing of terrorism.

6. Area – virtual currencies

Table no. 16

Type of services, financial products used	decentralised and exchangeable virtual currencies (so-called cryptocurrencies)
General risk description	usage of cryptocurrencies to transfer assets for the purposes of terrorist activity

[24] During all three audits conducted by the GIFI in the year 2017 at OI dealing in currency exchange, certain discrepancies were discovered.

[25] With the exclusion of services rendered by banks.

[26] Work is ongoing on a draft *act on amending the Polish act – Currency law as well as certain other acts*, spanning the coverage of entities exchanging currencies cashlessly by supervision. According to its assumptions „cashless currency exchange transactions conducted by on-line exchange agencies, and cash-cashless transactions of currency exchange" would be subordinate to the provisions of the *Polish act of August 19th, 2011, on payment services*. However, even now, some entities offering cashless currency exchange and payment services is supervised by the Polish Financial Supervision Authority.

[27] Poles exchange currencies on-line. Report – trends in currency exchange, first half of 2017, Xchanger and Fintek.pl, 2017, p. 2, at: https://fintek.pl/najnowszy-raport-kantorach-internetowych-polsce/.

Risk emergence scenario (e. g. possible example of the emergence of risk)	1. The dissemination of information about the addresses of cryptocurrencies, to which supporters of terrorist organisations transfer assets in decentralised and traded virtual currencies. 2. Collecting funds from supporters of terrorist organisations or unaware investors under the guise of financing of preparations to start up a new cryptocurrency, which emission either never takes place or ends with the depreciation of the released currency. The collected funds are transferred to a terrorist organisation. In addition, a system of references may work that serves the efficient recruitment of new members.
Vulnerability level	3
Vulnerability level substantiation	Access to these types of services is relatively easy. There are possibilities of hiding customer identification data (entities offering these kinds of services perform customer identification remotely). International transactions do arise. Entities offering services in the area of virtual currency exchange (including cryptocurrencies) or making so-called „hot wallets" available are OI. However offers of entities registered abroad, even outside of the EU, which are not subject to obligations in terms of countering ML/TF, are available online. Additionally, transactions using cryptocurrencies may be performed without the intermediation of third parties. Public authorities possess basic knowledge on ML/TF risk in this regard. The GIFI has the capacity to collect and analyse information on these kinds of services, however, stemming from entities that are OI or provided by foreign Financial Intelligence Units. There exists the possibility that a case of TF in the form of the analysed scenarios would not be detected. The level of domestic and international cooperation of public administration bodies is relatively good. Existing legal provisions partly correspond to the scope of the analysed risk.
Threat level	2
Threat level substantiation	Usage of cryptocurrencies to transfer asset values for purposes of terrorist activity can be a method of financial support of terrorism due to their properties facilitating the anonymization of parties to the transaction, and hindering both tracking of transfers as well as stopping them. However, according to an analysis by EUROPOL of September 19th, 2017 (*Risk Analysis on the use of Virtual Currencies for Terrorism Financing purposes*), even though virtual currencies have gained popularity due to the key properties such as global availability, ease of access, reliable and irreversible transactions, low costs and speed of international transfer, the development of their popularity among terrorist organisations seems to be relatively week as compared to the development of their popularity in supranational organised crime, in particular those related to cybercrime. Foreign services have identified cases of usage of virtual currencies to conduct transactions related to financing of terrorism, however, their numbers remain relatively low.[28] The use of virtual currencies is difficult and requires specialised knowledge. CONCLUSION: The usage of virtual currencies to transfer assets for purposes of terrorist activity creates a medium-level threat of financing of terrorism.

7. Area - telecommunications services related to mobile payments

Table no. 17

[28] A terse note on this subject may be found in: „European Union Terrorism Situation and Trend Report 2019". pp. 17-18 (at: https://www.europol.europa.eu/activities-services/main-reports/terrorism-situation-and-trend-report-2019-te-sat).
Some cases of use of virtual currencies for terrorism financing were presented in the domestic assessment of terrorism financing in the United States: „National Financing of Terrorism Risk Assessment 2018", pp. 26-27 (at: https://home.treasury.gov/system/files/136/2018ntfra_12182018.pdf). It notes, however, that virtual currencies do not constitute a significant risk of financing of terrorism.

Type of services, financial products used	payments made by mobile phones
General risk description	purchasing or topping up SIM cards to transfer funds
Risk emergence scenario (e. g. possible example of the emergence of risk)	Using mobile payments that fail to sufficiently apply customer due diligence measures, for the purpose of financing of terrorism in a manner hindering the identification of the originator and beneficiary of the transaction, e. g. supporters of a terrorist organisation transfer mobile payments (debiting their phone bills) for the benefit of a single person, who then withdraws the money received at a cash machine in order to transfer them for use by a terrorist organisation.
Vulnerability level	4
Vulnerability level substantiation	The possibility of offering these types of services as well as access to them is relatively easy. There exists the possibility of hiding customer identification data (when using straw men or possibly foreign phone numbers). International transactions can possibly arise. Entities offering such services are not OI. Public authorities possess basic knowledge on ML/TF risk in this regard. The GIFI is unable to collect and analyse information on these kinds of services. There exists the possibility that a case of TF in the form of the analysed scenarios would not be detected. The level of domestic and international cooperation of public administration bodies is relatively good. Existing legal provisions mostly do not correspond to the scope of the analysed risk.
Threat level	1
Threat level substantiation	Purchasing or topping up SIM cards to transfer assets is one of the more secure and fast ways to finance terrorist activity. The use of mobile payment systems that do not sufficiently apply customer due diligence measures is cheap and attractive. All it takes is to switch on within a mobile app of the option of transfers to a phone number or to transfer resources to a beneficiary for withdrawal from an ATM. In Poland, however, there is no clear information on the use of this *modus operandi* for the financing of terrorist activity. A reduction of the anonymity of this option is the obligation to register prepaid numbers introduced in 2017 so that each phone number would have their clearly identified user. CONCLUSION: The use of purchases or top-ups of SIM cards to transfer/collect resources for terrorist activity constitutes a low threat of financing of terrorism.

Table no. 18

Type of services, financial products used	telecommunications services concerning premium-rate phone numbers
General risk description	usage of telecommunications services concerning premium-rate phone numbers to collect funds for terrorist activity
Risk emergence scenario (e. g. possible example of the emergence of risk)	The conclusion of a contract concerning the provision of telecommunications services concerning registered premium-rate phone numbers for the benefit of straw men in order to ensure perpetrator anonymity. Then, through the usage of appropriate codes, specific connections are made by supporters of a terrorist organisation, for which high rates are charged. Some of the profit achieved is payment for the "straw man", with the remaining majority being transferred for the purposes of terrorist activity.
Vulnerability level	4
Vulnerability level substantiation	The possibility of offering these types of services as well as access to them is relatively easy. There exists the possibility of hiding customer identification data (when using straw men or possibly foreign phone numbers). International transactions can possibly arise. Entities offering such services are not OI. Public authorities possess basic knowledge on ML/TF risk in this regard. The GIFI is unable to collect and analyse information on these kinds of services. There exists the possibility that a case of TF in the form of the analysed scenarios would not be detected. The level of domestic and international cooperation of public administration bodies is relatively good.

	Existing legal provisions mostly do not correspond to the scope of the analysed risk.
Threat level	2
Threat level substantiation	Usage of telecommunications services spanning premium-rate phone numbers to collect funds for terrorist activity is an identified form of financing of terrorism. Even though there is no clear information in Poland about the use of this *modus operandi*, the Polish Internal Security Agency had in the past found cases of foreigners from elevated-risk states engaging in telecommunications fraud with PREMIUM-type numbers, the proceeds from which were most probably used for the operation of terrorist groups. This mode is perceived as relatively attractive for the purposes of financing of terrorist activity, a distributed group of supporters or persons supporting terrorist activity can easily support/provide low-amount transfers to an entity offering telecommunications services spanning premium-rate numbers. The proceeds from such activity are foreseen for terrorist activity. Planning, knowledge and skills are required, however, to use this *modus operandi*. In addition, this is not a cheap mode. CONCLUSION: The use of telecommunications services spanning premium-rate phone numbers to collect funds for terrorist activity creates a medium-level threat of financing of terrorism.

8. Area - physical transfer of asset funds

Table no. 19

Type of services, financial products used	cash couriers
General risk description	usage of natural persons for the transfer of cash across state borders
Risk emergence scenario (e. g. possible example of the emergence of risk)	1. Natural persons (sometimes only contracted for the purpose of one-time transport of assets) transport these funds across borders in various manners: • making one-time transports of cash below the obligatory declaration threshold, • declaring the import/export of cash above the threshold value and indicating a fictitious purpose of their use, • transporting/smuggling cash, hidden in luggage, in the transport resource/ vehicle, under clothing. 2. Beside cash, transported may also be value assets such as precious stones and metals, works of art, payment cards, prepaid cards, cheques, etc. 3. The transport of high amounts of money while declaring the import/exports of an amount slightly above the threshold foreseen by cash transport declarations that would not arouse suspicion. Perpetrators hope that customs or border officials will stop the moment their duty is fulfilled when the declaration is made and would not be looking for other financial assets of a higher amount transported by the perpetrators.
Vulnerability level	4

Vulnerability level substantiation	Access to transfer of cash funds is very easy – anyone can be such a courier. During inspections on outside borders of the EU it is not possible to hide the identification data of the courier. However, the transport of cash resources, and at the same time the identification data of the courier, need not necessarily be detected by public authorities at the border. Entities offering such services are not OI. Public administration authorities have knowledge on ML/TF risk in this regard. The GIFI is able to collect and analyse information (information provided by National Revenue Administration and the Polish Border Guard). The probability is high that a case of TF is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of domestic and international cooperation of public administration bodies is relatively good. Existing legal provisions mostly correspond to the scope of the analysed risk.
Threat level	3
Threat level substantiation	The usage of natural persons to transport cash across state borders is one of the most frequently seen methods of financing of terrorist activity. The transport of cash or other assets across state borders is a broadly available mode, and its use costs relatively little and is perceived by perpetrators to be attractive and relatively safe, in particular if the transported amounts are below the threshold of obligatory transport declaration. The usage of natural persons to transport money from illegal sources across state borders does not require specialised knowledge or skills, and ensures anonymity for the criminal group organising the procedure. The GIFI has received limited information about the possibility of usage of this method for the financing of terrorist activity. Polish services have noted cases of usage of this method to transfer assets foreseen for terrorist activity. CONCLUSION: The usage of natural persons to transport cash across state borders constitutes a high threat of financing of terrorism.

Table no. 20

Type of services, financial products used	courier, postal packages; cargo transport
General risk description	usage of courier and postal services
Risk emergence scenario (e. g. possible example of the emergence of risk)	A supporter of a terrorist organisation transfers assets collected for its needs in packages sent by post to a natural person residing in a country neighbouring a region of terrorist activity, which then transfers the received funds to members of this organisation.
Vulnerability level	3
Vulnerability level substantiation	Access to courier and postal services as well as cargo transport is relatively easy. There are possibilities of hiding the identification data of parties ordering and receiving the shipments. Courier and postal packages as well as goods in cargo services are transported between persons and entities from various countries. Only a part of entities offering these services are OI. These do not include transport companies or forwarders. Public authorities have limited knowledge on the ML/TF risk in this regard. The GIFI is able to collect and analyse information solely in a limited manner. The probability is high that a case of TF in the form of the analysed scenarios would not be detected. The level of domestic and international cooperation of public administration bodies is relatively good. Existing legal provisions only partially correspond to the scope of the analysed risk.
Threat level	2

Threat level substantiation	The usage of courier and postal services to transfer assets to terrorist organisations for the purposes of terrorist activity is an identified method of financing of terrorism. It is a mode that is relatively simple to use, it is broadly available, it costs relatively little to use it and it is perceived by perpetrators to be rather attractive. The use of delivery or postal services usually does not raise suspicions. The high volume of circulation in terms of international post permits the hiding of usage of these services for the transport of cash for purposes of terrorist activity, in particular if the individual amounts are not too high. In order to hide the actual beneficiary, 'straw men' are frequently used. The usage of this *modus operandi* requires, however, planning, knowledge of the postal system and logistical skills. The GIFI has received very limited information about the possibility of usage of this method for the financing of terrorist activity. CONCLUSION: The usage of courier, postal packages, cargo transport constitutes a medium-level threat of financing of terrorism.

9. Area – gambling

Table no. 21

Type of services, financial products used	on-line gambling
General risk description	resources acquired for the promotion of terrorism were laundered with the use of on-line gambling
Risk emergence scenario (e. g. possible example of the emergence of risk)	1. Criminals would "hack" credit cards, and then launder resources obtained from the accounts of these cards using on-line gambling to use them later as payments for websites promoting the struggle and 'martyrdom' of terrorists, and which were also used to facilitate contacts between terrorists and convey information on the mode of production of bombs. 2. Usage of on-line gambling sites to launder money from forbidden activity, such as fraud. A person supporting terrorist groups transfers assets to a relevant bank account related to an on-line gambling platform. The resources are transferred back to the subject platform customer as 'winnings' and then used for financing of terrorism.
Vulnerability level	2
Vulnerability level substantiation	Access to on-line gambling is relatively easy, as new sites offering gambling continue to emerge. In case of foreign *on-line* casinos it is easy to hide the identification data of the player. International transactions are possible, in particular when making financial transactions, as the bank accounts of entities offering on-line gambling are placed abroad. Nonetheless, the National Revenue Administration (NRA) in cooperation with the Polish Financial Supervision Authority (FSA) have developed rules concerning limiting the use of payment instruments or services offered by payment service providers in Poland to make transactions related to illegal gambling. Hosting providers in turn remove/ block access to forbidden content related to illegal on-line gambling. In December of 2018, the first Polish (legal) *on-line* casino was opened. Payments may only be done by on-line transfers or the Blik system. All entities offering gambling are OI. They possess a certain awareness of their obligations in terms of AML/CTF, even though shortcomings continue to be revealed in terms of their execution.[29] Relatively limited information about suspicious transactions/activity is transferred by entities offering on-line gambling (in the year 2017 this was 0.00% of all SARs from OI and 0.008% of all STRs) – as compared to other OI. Public administration authorities have knowledge on ML/TF risk in this regard. The GIFI is able to collect and analyse information. The probability is high that a

[29] In the years 2017-2018, six out of 10 audits by the GIFI of entities offering gambling revealed irregularities in terms of fulfilment of obligations in the area of combating money laundering and financing of terrorism.

	case of TF is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of domestic and international cooperation of public administration bodies is relatively good. Existing legal provisions mostly correspond to the scope of the analysed risk.
Threat level	1
Threat level substantiation	The usage of on-line gambling can be a method of usage of illegally-acquired funds for the purposes of financing of terrorism. However, according to Polish provisions, offering gambling via the Internet, save for mutual betting and promotional sweepstakes, is covered by monopoly of the state. Legal provisions forbid both gabling via the Internet by entities not authorised for this purpose as well as the participation in such games. The control activity of the NRA, the establishment of the register of domains used for offering gambling contrary to the law and limiting access to forbidden Internet domains can negatively influence the possibility of using illegally-acquired funds for financing terrorism. The GIFI has not received information about the possibility of usage in Poland of the *modus operandi* entailing the usage of on-line gambling for financing of terrorism. Due to the legal provisions, this *modus operandi* seems to be perceived by perpetrators as being unattractive and relatively risky for the purpose of legalisation of assets from forbidden activity. In addition, the use of this *modus operandi* requires planning, knowledge and skills. CONCLUSION: The use of on-line gambling constitutes a low threat of financing of terrorism.

10. Area – non-profit organisations

Table no. 22

Type of services, financial products used	charity activity
General risk description	usage of funds collected for charity purposes to finance terrorist organisations
Risk emergence scenario (e. g. possible example of the emergence of risk)	1. Usage of charity organisations controlled by terrorists (both registered and unregistered) to collect and transfer money for terrorist organisations. 2. Usage of funds for financing of terrorism by persons acting as part of non-profit organisations – during collection, meaning, before the funds are deposited on the account of the organisation. 3. A supporter of a terrorist group, having access to money collected by a legal charity as its employee, responsible for their accounting or supervision in this regard, facilitates their transfer for this terrorist organisation. 4. Supporters of terrorist groups acting as legally operating charity organisations and the collection of funds under fictitious references in order to transfer them to these groups. 5. Within a charity organisation controlled by supporters of terrorist groups, funds collected for humanitarian purposes are mixed with resources collected for terrorist purposes, to hide them and transfer them in an easier manner to these terrorist groups. 6. Resources collected for legal charity purposes – sent to their destinations in conflict zones or in their vicinity – are taken over by terrorist organisations for their own purposes. 7. Suppliers of asset transfer services taking a 'tax' for the transfer of funds from these organisations to the destination area. The 'tax' is then transferred to the terrorist organisation active in the relevant region. 8. Transfer by non-profit organisations of resources from donors to foreign non-profit organisations that use the received assets for financing of terrorism.
Vulnerability level	3
Vulnerability level substantiation	It is difficult to establish a foundation or association (specific duties need to be fulfilled, e. g. drawing up the bylaws, registration with the Polish National Court

	Register, additionally one must expect to be controlled by public authorities). It is easy to hide the identification data of real donors and beneficiaries, in particular if the foundation or association is controlled by perpetrators. International transactions are possible. Foundations and associations having legal personality are OI only in the scope, in which they accept or make payments in cash in a value equal to or exceeding the value of 10,000 Euro or equivalent, irrespective of whether the payment is effected as a single operation or several operations that seem mutually related. The above mentioned entities have a certain awareness of their duties in terms of AML/CTF, even though shortcomings continue to be revealed in terms of their execution.[30] They do not provide information about suspicious transactions/ activity to the GIFI (in 2017[31] there were no STRs or SARs from them) or transfer relatively limited information. Public administration authorities have knowledge on ML/TF risk in this regard. The GIFI is able to collect and analyse information. The probability is high that a case of TF is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigations. The level of domestic and international cooperation of public administration bodies is relatively good. Existing legal provisions mostly correspond to the scope of the analysed risk.
Threat level	2
Threat level substantiation	Charity organisations can be used by terrorist groups for their financing in various ways. This may entail direct transfer of a part of resources acquired by non-profit organisations for purposes of terrorist activity or the transfer of all funds collected by a non-profit organisation if the organisation is just a front for terrorist activity. The charity organisation can also operate actual charity work, however, aid is provided by entities within the organisation that are controlled by members related to terrorist groups. This leads to the situation in which the beneficiaries of the aid are convinced that they are receiving support from a terrorist organisation. Such activity provides significant propaganda advantages. Non-profit organisations are used by terrorist organisations, as thanks to charity work they enjoy significant public trust. The content provided by non-profit organisations greatly influences human attitudes, and any possible opposition by authorities can be met with accusations of persecution, racism or human rights violations. The use of this *modus operandi* itself is seen for the above reasons as being quite attractive and safe. The preparation of logistics for such operations requires a medium level of preparation. The GIFI has received limited information about the possibility of usage of this method for the financing of terrorist activity. CONCLUSION: The usage of charity organisations for financing of terrorism in Poland constitutes a medium threat of financing terrorism.

11. Area – crowdfunding

Table no. 23

Type of services, financial products used	crowdfunding
General risk description	acquisition of donors for terrorist organisations using modern communications networks

[30] In the years 2017-2018, three out of three audits conducted by the GIFI at foundations revealed irregularities in terms of fulfilment of obligations in the area of combating money laundering and financing of terrorism.

[31] At that time, all foundations were OI, irrespective of the cash payments accepted or made, as well as associations with legal personality accepting payments in cash equal to or higher than the equivalent of 15,000 Euro, also by way of more than a single operation.

Risk emergence scenario (e. g. possible example of the emergence of risk)	1. Organising events via *crowdfundig* platforms to collect resources for terrorist activity. The actual objective of the collection of funds will not directly indicate to the will to use the collected funds to finance terrorism. 2. Supporters of a terrorist organisation send out call for providing funds via social media. Donors transfer resources to the initiators in cash or buy international prepaid cards, the numbers of which are then provided to these.
Vulnerability level	4
Vulnerability level substantiation	It is fairly easy to start up a crowdfunding drive, e. g. via social media. It is easy to hide the identification data of donors and beneficiaries. International transactions are possible. In theory, anybody can run a crowdfunding drive. Entities organising such events are not OI. Public authorities possess basic knowledge on ML/TF risk in this regard. The GIFI has limited capacity to collect and analyse information on such events. There exists the possibility that a case of TF within the scope of the analysed scenario goes undetected. The level of domestic and international cooperation of public administration bodies is relatively good. Existing legal provisions do not correspond to the scope of the analysed risk.
Threat level	2
Threat level substantiation	Crowdfunding constitutes an alternative source of financing, including for terrorist activity. It is a form of financing of diverse kinds of projects by the community that is or will be organised around these projects. Terrorist activity as a certain kind of undertaking is, in such a case, financed by a large number of minor, one-time payments made by persons interested in supporting terrorist activity. Usually, however, the objective of such a fund drive is not clearly presented. *Crowdfunding* costs relatively little, and can be perceived by perpetrators as a *modus operandi* that is relatively attractive and broadly available for financing of terrorism, this is, however, burdened by significant risk. Usually, crowdfunding drives last a certain time, hence, *crowdfunding* is fairly easy to pinpoint and might not necessarily bring the desired results, a fact that influences the perception of this method as being of relatively limited attractiveness. The GIFI has received very limited information on the possibility of usage of this method for the financing of terrorist activity. CONCLUSION: Usage of crowdfunding constitutes a medium-level threat of financing of terrorism.

12. Area – trade in high-value goods

Table no. 24

Type of services, financial products used	precious stones and metals
General risk description	precious stones and metals taken by terrorists are smuggled to other countries for the purpose of their sale
Risk emergence scenario (e. g. possible example of the emergence of risk)	1. The bank account of company C was credited with relatively high amounts of cash from entities dealing in diamond trade. This money was then transferred to the Middle East for the benefit of a citizen of an European country – one A, originally from Africa. Some resources were transferred via the account of one of the board members of company C. The money was exchanged into EUR and then transferred to the benefit of Mr B. Mr A and Mr B bought diamonds from rebels active in an African country, and then smuggled them to Europe. 2. Purchase by a Polish company of precious metals such as gold, from a foreign company being an intermediary in the transfer of this metal. Precious metals may stem from areas covered by activity of terrorist groups, and assets obtained from their sale may be used for their financing.
Vulnerability level	3

Vulnerability level substantiation	Inasmuch as the purchase and sale of relatively small volumes of such goods is no trouble (e. g. at jewellers'), the purchase/sale of large/wholesale volumes is. However, it is easy to avoid identification, in particular when purchasing/selling goods at a value below the equivalent of 15,000 Euro. It is possible to buy/sell online, and hence, to conduct international transactions (e. g. when purchasing gems or metals from a foreign entity). Presently, entities dealing in the trade in metals or precious or semi-precious gems are not OI, as long as they do not accept or make payments for goods in cash with a value equivalent to or exceeding 10,000 Euro, irrespective of whether the payment is effected as a single operation or several operations that seem mutually related. It is possible to buy gold as bars in Poland, as well as gold coins – so-called bullion coins (without numismatic value). Additionally, bullion coins are treated as legal tender, a fact that ensures the possibility of transporting coins between countries. In addition, the import, processing and trade in diamonds is not legally regimented in Poland. Public administration authorities have knowledge on ML/TF risk in this regard. The GIFI is able to collect and analyse information. The probability is high that a case of TF is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of domestic and international cooperation of public administration bodies is relatively good. Existing legal provisions mostly correspond to the scope of the analysed risk.
Threat level	1
Threat level substantiation	The usage of trade in precious stones and metals robbed by terrorists is an identified method of financing of terrorism. Precious stones or metals are smuggled by terrorist organisations from war zones, where these organisations are active, to other countries, for the purpose of their sale in order to finance terrorist activity. However, this mode of financing frequently requires drawing up fake certificates of origin for the goods being sold. It is not entirely safe, as it may give rise to interest of services in the country of sale. The use of this *modus operandi* requires knowledge of the local market, planning and specialised knowledge. There is no information about the possibility of usage of this method for the financing of terrorist activity in Poland. CONCLUSION: The usage of the mechanism of purchase of precious stones and metals from persons related to terrorist activity for financing of terrorism creates a low level of threat in Poland.

Table no. 25

Type of services, financial products used	antiques and works of art
General risk description	purchase of stolen antiques and works of art from persons related to terrorist activity
Risk emergence scenario (e. g. possible example of the emergence of risk)	Purchase by Polish collectors of works of art and antiques stemming from areas covered by activity of terrorist organisations (e. g. the Middle East). The purchased goods might have been illegally taken from the owners by the terrorist organisation in order to finance their activity.
Vulnerability level	3

Vulnerability level substantiation	The purchase/sale of antiques or works of art is relatively easy. There are many companies trading in such goods on the basis of the Polish *act – Entrepreneur law* (auction houses, antiquarian stores). It is easy to avoid identification, in particular when purchasing/selling goods of a value below the equivalent of 15,000 Euro. It is possible to buy/sell online, and hence, to conduct international transactions. Presently, auction houses or antiquarian stores are not OI, as long as they do not accept or make payments for goods in cash with a value equivalent to or exceeding 10,000 Euro, irrespective of whether the payment is effected as a single operation or several operations that seem mutually related. Public administration authorities have knowledge on ML/TF risk in this regard. The GIFI is able to collect and analyse information. The probability is high that a case of TF is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigations. The level of domestic and international cooperation of public administration bodies is relatively good. Existing legal provisions mostly correspond to the scope of the analysed risk.
Threat level	1
Threat level substantiation	The usage of the mechanism of purchase of stolen antiques and works of art from persons related to terrorist activity is a mode of financing of terrorist activity. In Poland, the climax of vulnerability to this mechanism was during the participation of the Polish military during the operation in Iraq. This is, however, a method of financing of terrorism that is difficult to use. It requires considerable logistical effort, specialist expert opinions, knowledge of the art market, knowledge of customers ready to pay for black-market goods, and every trade operation should remain discrete. It frequently requires drawing up fraudulent certificates of origin for the sold antiques and works of art. The conducted financial operations may always raise suspicions in terms of their legality. The usage of this *modus operandi* requires planning and highly specialised knowledge. Information is lacking about the possibility of usage of this method for the financing of terrorist activity in Poland. CONCLUSION: The usage of the mechanism of purchase of stolen antiques and works of art from persons related to terrorist activity for financing of terrorism creates a low level of threat in Poland.

13. Area – business (general)

Table no. 26

Type of services, financial products used	legal business operation
General risk description	usage of active business entities for financing of terrorism
Risk emergence scenario (e. g. possible example of the emergence of risk)	1. Company X active on the used car market finances terrorism from proceeds acquired from the sale of cars. 2. Financing of activity of terrorist organisations using profit achieved by a company dealing in leasing and trade in real estate. 3. Purposeful fusion of resources acquired from sponsors of a terrorist organisation with the legal revenue of a business entity dealing in international trade to hinder the identification of the activity of financing of terrorism.
Vulnerability level	2
Vulnerability level substantiation	The formation of a company under the Polish *law on companies* or starting business activity as a natural person conducting business is to a certain extent limited by provisions of the law, requiring registration and the fulfilment of certain conditions (e. g. for capital and share-based limited partnerships – holding the company capital in a specific volume). Naturally, there are ways to hide the data of the beneficial owner through the use of straw men or shell companies. The introduction of foundation capital or the purchase/ sale of an existing entity may

	be effected by way of an international financial transaction, but also with participation of persons/foreign entities Only a part of the businesses entities are OI. Public administration authorities have knowledge on ML/TF risk in this regard. The GIFI has limited capacity to collect and analyse information. The probability is high that a case of TF is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/ investigation. The level of domestic and international cooperation of public administration bodies is relatively good. Existing legal provisions mostly correspond to the scope of the analysed risk.
Threat level	2
Threat level substantiation	The usage of active businesses for the financing of terrorism is one of the basic modes of financing of terrorist activity. Legally operating companies operate to benefit terrorist activities, and a part or the entirety of profit of these companies is transferred to terrorist activity. These companies are usually found in industries related to real estate trade, trade in electronics, used cars, precious metals, textiles, the export and import of food as well as gastronomic services. Legal businesses may be used both directly to acquire funds to support terrorist activity as well as conveyor belts to transfer funds related to the financing of such activity. Frequently, the legal assets of a business entity are mixed with assets from sources financing terrorism and moved on, in order to hinder the identification of assets as financing terrorism. Frequently, businesses operating legally dealing with the transfer of resources related to financing of terrorism are operated by members of a single ethnic group, raising the level of difficulty in disclosing this situation. This is a mode that is relatively easy to apply and broadly available, it costs relatively little to use it and it can be perceived by perpetrators as being rather attractive. The use of actual businesses for financing of terrorism usually does not raise suspicions. The high volume of trade of the subject companies permits the usage of these companies for the transfer of money for purposes of terrorist activity to remain hidden, in particular if the individual amounts are not too high. In order to hide the beneficial owner, counterfeit transaction documentation is frequently used. The use of this *modus operandi*, however, requires planning, accounting knowledge and logistical skills. The GIFI had received limited information about the possibility of usage of this method for the financing of terrorist activity. CONCLUSION: The usage of existing businesses for financing of terrorism creates a medium level of threat in Poland.

Table no. 27

Type of services, financial products used	shell companies
General risk description	usage of companies that in practice do not run their business for terrorism financing
Risk emergence scenario (e. g. possible example of the emergence of risk)	1. The purchase of companies that used to operate businesses for the purpose of using them to hinder identification of the transfer of asset values for the purpose of financing of terrorism. 2. Provision of accounting and administration services for the benefit of a limited liability company belonging to a foreigner by a Polish business specialising in corporate services. Usage of the discussed limited liability company for financing of terrorism. 3. Perpetrators create complex and long chains of organisational and ownership tiles between economic entities, associations, charity organisations, trusts (with the participation of various entities registered in various systems, e. g. tax havens) in order to make identification of the actual owners of entities used for financing of terrorism difficult. 4. Transfer of value assets between the above described businesses under various reference titles (e. g. purchase/sale of goods and services, number of shares, provision/repayment of loans) in order to finance terrorist needs.
Vulnerability level	2

Vulnerability level substantiation	The establishment of a company within the commercial code or the commencement of business as a sole proprietor is to a certain extent limited by provisions of the law, requiring these to be registered, and the fulfilment of certain conditions (e. g. for capital companies and a limited joint stock partnership– holding company capital in an appropriate volume). It is possible to hide data of the beneficial owner by means of straw men or shell companies. The contribution of founding capital or the purchase/acquisition of an existing entity may also be performed by way of an international financial transaction or with the participation of foreign persons/entities. Only some of these entities are OI. Public administration authorities have knowledge on ML/TF risk in this regard. The GIFI has limited capacity to collect and analyse information. The probability is high that a case of TF is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/ investigation. The level of domestic and international cooperation of public administration bodies is relatively good. Existing legal provisions mostly correspond to the scope of the analysed risk.
Threat level	2
Threat level substantiation	The usage of companies that in practice do not perform business operations is one of the fundamental modes of the transfer of funds related to financing of terrorist activity. Legally established businesses that are practically inactive operate several accounts that function only as conveyor belts to transfer financial resources to the benefit of terrorist organisations. The cash deposits or transfers for the company are in place to serve the obfuscation of the origin of the funds that are conveyed further, frequently to accounts of other entities found in more sensitive regions in terms of countering terrorism. Frequently, these businesses operating only seemingly and dealing with the transfer of assets related to financing of terrorism are operated by members of a single ethnic group, influencing difficulty in disclosing this *modus operandi*. The usage of companies that in practice do not conduct business to transfer funds related to the financing of terrorist activity is a simple and broadly available mode, and it costs little to use; it may rather be perceived by perpetrators to be fairly attractive. The use of existing business entities to finance terrorism usually raises no suspicions, however, the threat may be found in the non-standard approach of these companies in the business terms that is sometimes seen. In order to hide the beneficial owner, counterfeit transaction documentation is frequently used. The use of this *modus operandi*, however, requires planning, accounting knowledge and logistical skills. The GIFI has received limited information about the possibility of usage of this method for the financing of terrorist activity. CONCLUSION: The usage of companies that in practice do not conduct business for financing of terrorism creates a medium-level threat in Poland.

14. Area – social aid

Table no. 28

Type of services, financial products used	pensions, benefits and old age support
General risk description	usage of social aid by foreign terrorist fighters
Risk emergence scenario (e. g. possible example of the emergence of risk)	Usage of social aid (received legally or fraudulently) to pay travel and accommodation costs for foreign terrorist fighters in conflict zones.
Vulnerability level	3
Vulnerability level substantiation	The reception of such aid necessitates the satisfaction of certain legal criteria. It is difficult to hide the identification data of beneficiaries. International transfers are possible (e. g. the movement of pension payments, retirement aid, benefits for entitled persons operating accounts abroad). The authorities that assign old age/ retirement/other benefits are cooperating entities. However, their level of awareness of their obligations in terms of AML/CTF may not be sufficient.

	Public authorities have basic knowledge on the risk of ML/TF in this regard. The GIFI has limited capacity to collect and analyse information on the provision of pensions/benefits and old age support. There exists the risk that a case of TF in the span of the analysed scenarios is not discovered. The level of domestic and international cooperation of public administration bodies is relatively good. Existing legal provisions mostly correspond to the scope of the analysed risk.
Threat level	1
Threat level substantiation	The usage of social aid by foreign terrorist fighters in Poland (e. g. to fund travel and accommodation of foreign fighters in the conflict zones) is quite a difficult mode of financing of terrorist activity. The amount of benefits for a foreigner in Poland to cover their stay in Poland on their own is at most PLN 750/person per month, assuming that it is a single person, whereby a member of a four-person family can only be provided with PLN 375 per month.[32] At migrant camps, financial benefits are much lower. As seen from the above, due to their amounts, social aid in Poland are rather of limited use as financing of terrorism. Much higher social aid for migrants or refugees are offered by richer countries of Western Europe. The above mentioned method of financing terrorism in the form of paying for travel and accommodation of fighters in conflict zones cannot be used under Polish conditions, and it is also risky for perpetrators due to the identification procedures conducted by the authority providing the benefits and through audits of use of benefits. The is no information about the possibility of usage of this method for the financing of terrorist activity in Poland. CONCLUSION: The use of social aid by foreign terrorist fighters to finance terrorism creates a low level of threat in Poland.

[32] Source - https://udsc.gov.pl/uchodzcy-2/pomoc-socjalna/system-pomocy-socjalnej/rodzaje-przyznawanej-pomocy/, access on 21.06.2019.