Ministerstwo Finansów

ANNEX NO. 2
MONEY LAUNDERING 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 from illegal sources
Risk emergence scenario (e. g. possible example of the emergence of risk)	1. Collecting in the bank account of resources (through cash payments or transfers from other accounts), for the purpose of cash payouts 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. Usage of bank accounts kept for legitimately existing companies. The transfer of funds stemming from illegal sources by way of a chain of bank accounts belonging to related business entities, under fictional titles (e. g. payment for services or loans or their repayment), in order to separate them from their original source. 3. Usage of bank accounts created for straw men or companies not actually conducting business activity (shell companies) in order to make transactions using resources stemming from illegal sources. 4. Opening bank accounts in the name of foreign legal entities (in particular registered in tax havens) and then using these accounts for cash payments and withdrawals as well as transfers from and to foreign bank accounts to hide illegal sources of the funds used in these transactions. 5. Opening bank accounts by natural persons on the basis of fake identification documents. Usage of bank accounts to introduce resources from illegal sources to the banking system and to further transfer these.
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 use financial safety 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 financing of terrorism (ML/TF) in this regard. The GIFI is able to collect and analyse information. There exists the probability that a case of ML is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of national 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
Threat level substantiation	Carrying out transactions by way of the created bank accounts, both company as well as natural person accounts, is one of the methods of money laundering that is simplest to use. This mode is broadly available and it costs little to make use of it. Carrying out transactions on bank accounts does not require specialised knowledge or skills. The customer due diligence measures used by banks do in fact create a certain risk for entities depositing or transferring resources through bank accounts, however these are circumvented by way of using fake documents, the verification of which is difficult for the bank. The GIFI registers many cases of using bank accounts for money laundering. CONCLUSION: The use of a bank account to collect and transfer money from illegal sources creates a very high threat of money laundering.

Table no. 2

Type of services, financial products used	credits and loans

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 financing of terrorism and the transfer of information to GIFI). 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.

5 *Suspicious Transaction Report*.

6 *Suspicious Activity Report*.

General risk description	acquiring credits and loans and their repayment by resources stemming from illegal sources
Risk emergence scenario (e. g. possible example of the emergence of risk)	1. Acquiring consumer credits and loans that are then relatively quickly (before the credit/loan repayment deadline) repaid using resources stemming from illegal sources. 2. Acquiring loans to purchase property/real estate, often at inflated prices, through straw men. The resources from the loans are transferred to property/real estate sellers cooperating with the perpetrators. The loans are repaid with resources stemming from illegal sources.
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 credit 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 ML is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of national 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	The usage of the possibility of entering into a credit or loan contract and their subsequent repayment by resources stemming from illegal sources is perceived in Poland as quite an attractive money laundering method. In case of mortgage loans, the threat of these being used for money laundering is also based on the possibility to determine real estate prices different from market prices as well as the possibility of filing tax statements with various tax offices (depending on the stated place of residence). Criminals utilising this method are well-prepared to provide false documentation, and the limited material law of the

[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 usage 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.

	mortgage helps to hide the beneficial owner of the funds. Frequently, loan providers are entities with seats in so-called „tax havens". This *modus operandi*, however, requires planning and a certain level of knowledge and skills. The GIFI received information about this mode of money laundering being used. CONCLUSION: The conclusion either a credit or loan contract and the subsequent repayment using resources stemming from illegal sources constitutes a significant threat of money laundering.

Table no. 3

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 perpetrators of money laundering
Risk emergence scenario (e. g. possible example of the emergence of risk)	1. Anonymous prepaid cards are loaded by perpetrators using resources stemming from illegal sources. With the prepaid card account, transfers are then made to bank accounts of other people for payout in cash or further transfers. 2. Anonymous prepaid cards are provided by perpetrators with resources stemming from illegal sources. Purchases of diverse goods are made using prepaid cards, to then be sold on to other parties.
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 money laundering are anonymous prepaid cards offered in Poland, but issued by issuers from other EU countries. There exists the possibility of issue of 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 AML/ CTF procedures in force (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 probability that a case of ML is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of national 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	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 money laundering could apply primarily to these cards purchased by natural persons. This requires perpetrators to know the offers of foreign electronic money institutions. However, due to the relatively low limit values set out in directive 2018/843 in conjunction with the possibility to

[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.

	waive customer due diligence measures with respect to electronic money that every EU member state is obliged to apply, this mode may not seem very attractive to perpetrators. There is information, mainly from abroad, about the use of this *modus operandi* for ML. CONCLUSION: The usage of prepaid cards (issued by electronic money institutions from other EU countries) to hinder the identification of perpetrators of money laundering has a low level of threat of money laundering in Poland at the moment.

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 in particular to banks located in tax havens. 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 ML is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of national and international cooperation of public administration bodies is relatively good. Existing legal provisions mostly correspond to the scope of the analysed risk.
Threat level	4

[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 usage of financial safety measures, as well as the organisation of the process of countering money laundering and financing of terrorism and the transfer of information to GIFI). GIFI in turn during four out of five bank audits conducted in the years 2017-2018 revealed flaws in the execution of obligations in terms of combating money laundering and financing of terrorism.

Threat level substantiation	The usage of transfers to transfer financial resources to other jurisdictions is one of the most commonly seen methods of money laundering (there is information about it being used by criminals). It is a widely available mode of action, and its use costs relatively little. It is perceived by perpetrators as being very attractive. The usage of transfers to move funds to other jurisdictions does not require specialised knowledge or skills. Frequently used by organised crime, it may sometimes be related to corrupting a single bank employee or controlling the operation of an entire branch office or agency. Customer due diligence measures used by banks are avoided in this *modus operandi* through corruption of bank officials or fake documents, the verification of which is difficult for the bank, e. g. invoices. CONCLUSION: The usage of transfers to move funds to other jurisdictions creates a very high threat of money laundering.

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 financial resource transfer service providers to move funds from illegal sources
Risk emergence scenario (e. g. possible example of the emergence of risk)	1. Usage of money transfers to transfer funds from illegal sources abroad in order for these to be used in a different jurisdiction. 2. Usage of money transfers to receive funds stemming from illegal, foreign sources, in order for these to be subsequently withdrawn in cash.
Vulnerability level	2
Vulnerability level substantiation	Money transfer services are relatively easily available. There exists a limited possibility to hide identification data of originators and beneficiaries of money transfers in case of making occasional transactions below the threshold corresponding to 1,000 Euro or in case of usage of a straw man or a shell 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 [of] OI from the area of payment services. 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 possibility that a case of ML is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of national 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
Threat level substantiation	The use of providers of financial resource transfer services to move money – as money transfers – from illegal sources to other countries or in order to receive illegalfunds, is a method of money laundering that is used frequently. It is a broadly available mode, and it costs little to make use of it, and it is perceived by

[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 se of financial safety 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, 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.

	perpetrators as being attractive. A payment account owned by the payer is not necessary to make this kind of transfer. Straw men are frequently used to hide the beneficial owner. The use of service providers in the area of fund transfers to move money from illegal sources abroad does not require specialised knowledge. The GIFI has received information on this method being used for money laundering. CONCLUSION: The use of providers of financial resource transfer services to move money – as money transfers - from illegal sources abroad or in order to receive illegal funds creates a very high threat of money laundering.

Table no. 6

Type of services, financial products used	on-line payment services
General risk description	usage of on-line payment services by perpetrators to transfer funds from illegal activity
Risk emergence scenario (e. g. possible example of the emergence of risk)	1. Usage of on-line payment services by perpetrators to move funds from illegal sources from bank accounts, where they were collected, and then their "shifting" between various accounts opened with payment service providers, in order for these to ultimately be moved to a bank account belonging to a natural person or business entity controlled by the perpetrators. 2. A payment institution agent (or a payment institution employee), cooperating with the perpetrators, accepts from them the funds stemming from illegal sources, which they subsequently transfer to bank accounts indicated by them via cashless transfers, hiding their source and purpose. 3. A customer of a payment institution is provided with relatively small payments from natural and legal persons, which are the result of committing the predicate offence for money laundering. The payments are made both in cash as well as cashless money transfers, ordered via obliged institutions, which allow the acceptance of funds for the benefit of that payment institution customer. The transferred funds are then collectively moved to a bank or payment account with a different financial institution, belonging to that payment institution customer.
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 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 ML is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of national and international cooperation of public administration bodies is relatively good.

[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, as well as the organisation of the process of countering money laundering as well as financing

	Existing legal provisions mostly correspond to the scope of the analysed risk.
Threat level	3
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 method of money laundering, which the GIFI and other bodies have met as part of execution of their statutory duties. It is possible, for instance, to introduce fragmented parts of funds stemming from crime (as cash or cashlessly) and then transfer these collectively by way of a payment institution to the target bank or payment account. An overly high turnover volume may attract attention. There are also limits to the total value of transactions performed in a specific time. Difficulties may also emerge in terms of the possibility of contacting the operator, should issues arise. It is worth noting, however that the liberalisation of provisions introduced on the basis of directive no. 2015/2366[16] allows an ever greater range of services that may be provided by payment institutions and relatively low requirements for business, permitting the establishment of a payment institution (in particular a small payment institution) without excessive financial resources, which could facilitate the activity of criminals. This *modus operandi* requires medium-level planning, knowledge and skills. It would seem, however that it may be perceived by perpetrators as ever more attractive. The GIFI has information on this method being used for money laundering. CONCLUSION: The use of on-line payment services creates a high threat of money laundering.

Table no. 7

Type of services, financial products used	Hawala-type transfer systems
General risk description	usage of Hawala networks or other informal transfer systems to transfer funds from illegal sources

of terrorism and transferring information to the GIFI). However, 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.

[16] Meaning *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC* (OJEU L no. 337 of 23.12.2015, p. 35).

Risk emergence scenario (e. g. possible example of the emergence of risk)	1. Using entities offering illegal payment services to transfer funds from criminal activity. For instance, a person offering such services utilises their bank accounts, to which they pay money from their customers. The funds are then transferred to accounts of entities offering legal payment services. 2. International transfer of funds from the revenue of criminal organisations established by criminals from the same region of the world to a different.
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 probability that a case of ML within the scope of the analysed risk is not detected. The level of national 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	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 depositing 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. The usage of this *modus operandi* requires knowledge on the people offering such services. There are no numerous ethnic minorities in Poland, in which Hawala-type systems would be commonplace. CONCLUSION: The usage of the informal Hawala transfer system to move funds from illegal sources constitutes a low money laundering risk.

3. Area – insurance

Table no. 8

Type of services, financial products used	life insurance
General risk description	use of capacities offered by life insurance related to an investment fund
Risk emergence scenario (e. g. possible example of the emergence of risk)	Funds stemming from illegal sources are deposited by criminals as part of life insurance and endowment, or alternatively life insurance together with investment funds, as additional premiums, concluded for themselves or for their next of kin. In a little while, the resources from the premiums are withdrawn and transferred on to the bank account of the criminal or a person controlled by them.
Vulnerability level	2

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 is making 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 ML is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of national 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 utilisation of possibilities offered by life insurance related to investment funds to legitimise funds from criminal activity is an identified method of money laundering. The GIFI had received from obliged institutions and cooperating units information about the use of this *modus operandi*, but this method is perceived to be of limited attractiveness. This *modus operandi* requires planning, knowledge and skills to use. It requires the preparation and updates of documentation for the insurance. CONCLUSION: The use of possibilities offered by life insurance related to investment funds to legitimise resources from criminal activity constitutes a medium-level threat of money laundering.

4. Area – other financial institutions

Table no. 9

Type of services, financial products used	services on the FOREX market
General risk description	usage of a broker company operating on the FOREX market as a *market maker* to legitimise funds from illegal sources.
Risk emergence scenario (e. g. possible example of the emergence of risk)	A company legally operating on the FOREX market as a broker and *market maker*[17] is controlled by persons related to the criminals who secretly fund its activity. The criminals create accounts on the transaction platform operated by this company. Thanks to insider information and more competitive conditions received from their company they expand their capital that is disclosed to tax authorities as investment gains on the FOREX market.
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

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

	continue to be revealed in terms of their execution.[18] 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 ML is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of national 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	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 that is active on the FOREX market and controlled by criminals as a broker in the *market maker* model to legitimise funds from illegal sources is a money laundering method of low attractiveness. This *modus operandi* requires specialised knowledge about the currency exchange market, skills as well as planning. In the *market maker* model, the profits of investors from participation in the FOREX market are the broker's loss. They cannot incur losses constantly, as this gives rise to suspicions. There is information that this type of activity is used to commit predicate offences for money laundering. CONCLUSION: The usage of a brokerage house operating on the FOREX market as a *market maker* to legitimise funds from illegal sources gives rise to a medium-level threat of money laundering.

Table no. 10

Type of services, financial products used	investment fund share units
General risk description	purchase of investment fund share units for funds stemming from illegal sources
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

[18] 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 use of financial safety 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). 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.

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.[19] 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 ML is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of national 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	As investment funds vary by their level of risk and the related type of financial instrument, in which they invest their assets, the achieved profit/loss level per fund unit varies. These differences also stem from the time horizon of the investment and of its objectives. The GIFI had limited information about investing illegal financial resources in investment funds. This always requires the interested party to plan and for them to have skills and specialised knowledge about the stock market. The *modus operandi* of money laundering with the use of investment fund share unit purchases with funds stemming from illegal sources is, however, perceived as having little attractiveness. CONCLUSION: The purchase of share units in investment funds for resources stemming from illegal sources creates a medium-level threat of money laundering.

Table no. 11

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 transfer and legitimise funds from illegal sources
Risk emergence scenario (e. g. possible example of the emergence of risk)	1. Perpetrators deposit funds from illegal sources on the capital market via companies established in particular in tax havens. 2. Perpetrators use the cash account used to handle the security accounts, established for the benefit of a natural person or a legal person related to them, and treat it as a "splitter". The account is credited with funds from illegal sources, pending further transfer to bank accounts of other entities controlled by the perpetrators. 3. A securities account belonging to the person or the entity controlled by the criminals is used to purchase securities for cash stemming from illegal sources and collected on the cash account used to handle the above described account, and then to sell them further within a relatively short time. Possible losses from these transactions thus become the cost of legalising these funds.
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

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

	obligations in terms of AML/CTF, even though shortcomings continue to be revealed in terms of their execution.[20] 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 ML is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of national 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 GIFI possesses certain information about the use of this *modus operandi* by criminals. Deposits on cash accounts used to handle the security accounts, with subsequent diverse forms of investment operations using these resources or the disposal or transfer to a different account is pretending that the assets gained from criminal activity are indeed legit. This is related to the supposition that the resources found in the cash account used to handle the security market stem from financial operations conducted on the stock market. This *modus operandi* is perceived by the perpetrators as quite an attractive form of money laundering. The level of complication of the financial market is a large advantage for criminal activity aiming to launder money. The usage of securities and cash accounts used to handle them to transfer and legitimise sources requires specialised knowledge, skills as well as planning. CONCLUSION: The usage of securities accounts and cash accounts used to handle them for the purpose of transferring and legitimising funds from illegal sources constitutes a high threat of money laundering.

5. Area – currency exchange

Table no. 12

Type of services, financial products used	cash foreign currency exchange
General risk description	foreign currency exchange to hinder identification of money from crime
Risk emergence scenario (e. g. possible example of the emergence of risk)	1. Use by criminals of cash-based foreign currency exchange at exchange offices to make it more difficult for law enforcement authorities to retrace the transfer path of assets. Using "trusted" exchange offices that do not report suspicious transactions to the financial intelligence unit. 2. Exchanging the collected money from illegal sources against high-value banknotes in other currencies at exchange offices (commonly traded all over the world, e. g. EUR), in order to make it easier to transport them across state borders.
Vulnerability level	2

[20] 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.

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.[21] Relatively little information about suspicious transactions/activity is transferred by entities dealing in foreign currency exchange[22] (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 ML is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of national and international cooperation of public administration bodies is relatively good. Existing legal provisions correspond to the scope of the analysed risk.
Threat level	3
Threat level substantiation	The usage of the foreign currency exchange mechanism to hinder identification of funds from crime is one of the more frequently used methods of money laundering. It is a method that is easy, broadly accessible, and it costs little to make use of it, and it is perceived by perpetrators to be rather attractive. Currency exchange transactions below the registration threshold raise no suspicions, in particular if e. g. exchange office employees cooperate with the criminals. The high exchange office turnover volume permits the hiding of illegal funds among legal transactions. The GIFI has received information on this method being used for money laundering, especially in conjunction with other methods. CONCLUSION: The usage of the foreign currency exchange mechanism to hinder the identification of cash stemming from crime constitutes a high threat of money laundering.

Table no. 13

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[23] in order to reduce the volume of the cash resources carried.
Vulnerability level	2

[21] 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.

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

[23] On May 4th, 2016, the European Central Bank decided to stop issuing 500 EUR banknotes. The majority of national central banks of the Euro zone issued them until January 2019, with the Deutsche Bundesbank and the Österreichische Nationalbank – issuing them until April of 2019. Banknotes issued until that time remain in circulation.

Vulnerability level substantiation	Access to these types of currency exchange services is difficult and dependent on the OI having banknotes of such denominations. It is easy to hide the identification data of the person making the transaction, in particular if the individual transactions encompass relatively low amounts. It is not possible to perform international transactions. All entities offering such services are OI. They are aware 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. The probability is high that a case of ML is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of national and international cooperation of public administration bodies is relatively good. Existing legal provisions correspond to the scope of the analysed risk.
Threat level	3
Threat level substantiation	The usage of the mechanism of exchanging low-denomination banknotes against higher-denomination banknotes is one of the more frequently used methods of money laundering. Such operations are performed at banks, exchange offices, but post offices as well. It is a broadly available mode, and it costs little to make use of it, and it is perceived by perpetrators as being attractive. However, the safety of this method requires planning, adherence to the rule of making low-amount 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 offering such services. The GIFI has received information on this method being used for money laundering. CONCLUSION: The usage of the mechanism of exchange of low-denomination money against high-denomination banknotes constitutes a high threat of money laundering.

Table no. 14

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 criminals of 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 originator.
Vulnerability level	3

[24] 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 GIFI in the year 2017 at OI dealing in currency exchange, certain irregularities were discovered.

[25] 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.[26] Relatively little information about suspicious transactions/activity is transferred by entities dealing in foreign currency exchange[27] (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 ML is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of national and international cooperation of public administration bodies is relatively good. Existing legal provisions partly correspond to the scope of the analysed risk.[28]
Threat level	4
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 one of the methods of money laundering. According to estimates available on-line, in the first six months of 2017 ca. 35% of foreign currency exchange transactions took place on-line.[29] 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 money laundering. 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 usage of this *modus operandi* requires planning, knowledge and skills of a low level of complexity. It can be perceived by perpetrators as quite attractive and safe. The GIFI has received information on this method being used for money laundering. 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 very high threat of money laundering.

6. Area – virtual currencies

Table no. 15

Type of services, financial products used	decentralised and exchangeable virtual currencies (so-called cryptocurrencies)
General risk description	usage of cryptocurrencies to transfer funds from illegal sources

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

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

[28] 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 are supervised by the Polish Financial Supervision Authority.

[29] 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. Usage of cryptocurrencies (e. g. Bitcoin) to obtain profit from various kinds of crime, including extortion (e. g. as payment for deciphering data that was hacked on a computer), kidnappings (as ransom for releasing the kidnapped). 2. Usage of cryptocurrencies (e. g. Monero) to make payments for drugs purchased through darknet marketplaces. 3. Usage of cryptocurrencies to obfuscate the source of illegal proceeds (e. g. money transferred as a result of unauthorised access to victims' bank accounts are transferred to an account of an entity being the virtual currency exchange platform in order to purchase cryptocurrency units. The purchased cryptocurrency units are then transferred to an anonymous *offline* wallet.
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 probability that a case of ML in the form of the analysed scenarios would not be detected. The level of national and international cooperation of public administration bodies is relatively good. Existing legal provisions partly correspond to the scope of the analysed risk.
Threat level	3
Threat level substantiation	Usage of cryptocurrencies to transfer asset values from illegal sources may be a method of money laundering. The cause is that the natural properties of cryptocurrencies provide the possibility of hiding relatively easily the data of the parties to the transaction, and difficulties may arise with following the transfer path[30] and possibly stopping it. This supports their use by organised crime groups, in particular as such transactions are difficult to trade for law enforcement and tax authorities. However, in order to use the above described *modus operandi* for money laundering, sufficient planning is necessary, as well as the knowledge on how to use them. The GIFI possesses certain information on the possibility of using cryptocurrencies to transfer asset funds from illegal sources. CONCLUSION: The usage of cryptocurrencies to transfer asset funds from illegal sources constitutes a high threat of money laundering.

Table no. 16

Type of services, financial products used	centralised virtual currencies

[30] In particular when tools are used to intermix, confuse transactions to complicate relationships between them and their users (so-called *anomizers*).

General risk description	usage of centralised virtual currencies to transfer funds from illegal sources
Risk emergence scenario (e. g. possible example of the emergence of risk)	Criminals exchange money stemming from illegal sources into units of centralised virtual currencies (e. g. *Webmoney*, *Perfectmoney*) at an on-line exchange office performing these kinds of transactions. Then, units in these currencies are placed in an account opened with a foreign provider of services in terms of such fund transfers (of a similar type to payment services). Units of these currencies are transferred to other accounts opened within the same transaction system, and following their exchange – to a foreign bank account.
Vulnerability level	3
Vulnerability level substantiation	Access to these types of services is relatively easy – however few entities offer these kinds of currencies. There are possibilities of hiding customer identification data (Entities offering these kinds of services perform customer identification remotely). International transactions do arise. Entities offering these services 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. Public authorities possess basic knowledge on ML/TF risk in this regard. The GIFI has limited capacity to collect and analyse information on these kinds of services. There exists the probability that a case of ML in the form of the analysed scenarios would not be detected. The level of national 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	The usage of centralised virtual currencies to transfer asset funds from illegal sources may also be a method of money laundering. The global character of financial and capital markets causes the emergence of relatively simple capacities to exchange money from illegal sources into units of centralised virtual currencies and (as a result of several transactions) in the other directions using anonymisation of parties to the transaction and of properties making the tracking of transfers as well as halting them more difficult). To use the above described *modus operandi* for money laundering, however, appropriate planning and the knowledge of how to use it, are required. The GIFI only possesses very limited information on the possibility of using centralised virtual currencies to transfer asset funds from illegal sources. CONCLUSION: Presently, the usage of centralised virtual currencies to transfer asset funds from illegal sources creates a medium-level threat of money laundering.

7. Area – telecommunications services related to mobile payments

Table no. 17

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 legalise funds from criminal 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 criminals or related persons, for which high rates are charged. Some of the profit achieved is payment for the "mule", with the remaining majority being used by criminals as “laundered” money.
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 probability that a case of ML in the form of the analysed scenarios would not be detected. The level of national 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 legalise funds from criminal activity can be a method of money laundering. The GIFI had received limited information on the usage of this *modus operandi*, but this method is perceived to be of limited attractiveness and relatively risky. The entity providing telecommunications services spanning premium-rate phone numbers is obligated to convey statutorily required information to the register kept by the Chairman of the Polish office of Electronic Communications. Usage of this *modus operandi* requires planning, knowledge and skills. Additionally, this method is not cheap. CONCLUSION: The usage of telecommunications services spanning premium-rate phone numbers to legalise funds from criminal activity creates a medium-level threat of money laundering.

8. Area – physical transfer of asset funds across the border

Table no. 18

Type of services, financial products used	cash couriers
General risk description	usage of natural persons for the transfer of cash from illegal sources 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 fictional purpose of their use, • transporting/smuggling cash, hidden in luggage, in the transport resource/vehicle, under clothing. 2. Beside cash, transported may also be asset values 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 asset 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 asset funds, 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 Polish National Revenue Administration and the Border Guard). The probability is high that a case of ML is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigations. The level of national and international cooperation of public administration bodies is relatively good. Existing legal provisions mostly correspond to the scope of the analysed risk.
Threat level	4
Threat level substantiation	The usage of natural persons to transport cash from illegal sources over state borders is one of the most frequently seen methods of money laundering. It is a broadly available mode, its use costs relatively little and is perceived by perpetrators as being very attractive. 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 method is frequently used by organised crime, can be related to corruption among border guard officials. The GIFI has received information, in particular from cooperating units, about the possibility of usage of this method for money laundering. CONCLUSION: Usage of natural persons to transport money from illegal sources across state borders creates a very high threat of money laundering.

Table no. 19

Type of services, financial products used	courier, postal packages; cargo transport
General risk description	usage of courier and postal services to transport cash from illegal sources
Risk emergence scenario (e. g. possible example of the emergence of risk)	The criminal transports funds stemming from illegal sources in packages mailed by post to natural persons in other countries. Recipients of the funds then introduce this money to the financial system (e. g. depositing them in bank accounts) to invest them or to purchase goods that are then made available to criminals.
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 ML in the form of the analysed scenarios would not be detected. The level of national 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	3

Threat level substantiation	The usage of courier and postal services to transport cash from illegal sources is a relatively easy, broadly available method of money laundering, and it costs little to make use of it. It is rather perceived by perpetrators as being attractive. The use of courier or postal services usually raises no suspicion. The high volume of circulation in terms of international post allows hiding of usage of these services for the transport of cash from illegal sources. Straw men are frequently used in order to hide the beneficial owner. The usage of this *modus operandi* requires, however, planning, knowledge of the postal system and logistical skills. The GIFI has received information on this method being used for money laundering, especially in conjunction with other methods. CONCLUSION: The usage of courier and postal services to transport money from illegal sources constitutes a high threat of money laundering.

9. Area – gambling

Table no. 20

Type of services, financial products used	on-line gambling
General risk description	funds stemming from illegal sources are laundered using on-line gambling
Risk emergence scenario (e. g. possible example of the emergence of risk)	The usage of on-line gambling platforms for money laundering from forbidden activities such as fraud. The perpetrator pays the funds in (using cryptocurrencies or money already collected in a bank account that they control) to a suitable bank account tied to the gambling platform. The funds are transferred back to the mentioned platform customer as "winnings".
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 (PFSA) 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 legal 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.[31] 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 case of ML is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of international cooperation of public administration bodies is relatively good.

[31] 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.

	Existing legal provisions mostly correspond to the scope of the analysed risk.
Threat level	2
Threat level substantiation	The usage of on-line gambling can be a method of laundering money from illegal sources. However, according to Polish provisions, offering gambling via the Internet, save for mutual betting and promotional sweepstakes, is covered by monopoly of the state. One legal Polish on-line gambling casino operates in since December 2018. Legal provisions forbid both offering illegal gambling on the Internet by unauthorised entities as well as participation in such gambling. Despite the ban, however, the GIFI has received some information about the possibility of using this *modus operandi*, however, this method, due to the legal conditions, is perceived as having little attractiveness and being relatively risky, to legalise funds from forbidden activity. Additionally, usage of this *modus operandi* requires planning, skills and capabilities. This method is also not cheap. CONCLUSION: The use of on-line gambling for laundering funds from illegal sources creates a medium-level threat of money laundering.

Table no. 21

Type of services, financial products used	mutual betting
General risk description	usage of mutual betting to legalise funds from illegal sources
Risk emergence scenario (e. g. possible example of the emergence of risk)	The criminal, foreseeing the results of sports events, places bets with bookmakers using funds from illegal sources (frequently – to improve the chance of winning – diversifying the bets placed, using the cash to make various bets concerning various sports events). The winnings are their legal profit as confirmed by the bill received from the bookmaker.
Vulnerability level	2
Vulnerability level substantiation	Access to mutual betting is relatively easy. Two basic types of bookmakers exist: so-called brick-and-mortar bookmakers, meaning, companies operating fixed outlets (stores), where one can pay by cash or card to receive a specific coupon, and on-line bookmakers who operate on the Internet. It is easy to hide the identification data of an illegal gambler on-line, in particular when on-line payment services are used. It is possible to perform international transactions, in particular if financial transactions are made when the accounts of the entity offering on-line gambling services are opened abroad. The estimate of the Polish Ministry of Finance shows that the „grey area" in the area of mutual on-line betting in the year 2018 amounted to ca. 51%.[32] All entities offering legal 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.[33] Relatively limited information about suspicious transactions/activity is transferred by entities conducting activity in the area of gambling (in the year 2017 it 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 case of ML is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of national and international cooperation of public administration bodies is relatively good. Existing legal provisions mostly correspond to the scope of the analysed risk. Presently, an amendment is being discussed to the Polish fiscal penal code that

[32] https://www.senat.gov.pl/download/gfx/senat/pl/senatoswiadczenia/2045/09_071_2053_1_odp.pdf, access on 24.06.2019.

[33] 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.

	should reduce the share of the grey area in the market. Changes apply to penal fiscal liability for providers of financial services who take part in the transfer of funds from Polish gamblers to bookmakers operating without a licence of the Polish Minister of Finance.[34]
Threat level	3
Threat level substantiation	The use of mutual betting to legalise funds from illegal sources is a frequently used mode of money laundering. Falsified confirmations of winnings on bets are documents that may contribute to the legalisation of profit from criminal activity. This is a fairly simple, broadly available method, requiring only moderate specialised knowledge. Its usage really does not cost much, and it is perceived by the perpetrators as being rather attractive. When choosing this *modus operandi*, criminals often illegally influence the results of the events they bet on, such as sports events (or other events being bet on). Straw men are also frequently used to hide the beneficial owner. The use of this *modus operandi*, however, requires planning, knowledge of the bet odds system (or influencing the correctness of evaluation of the emergence of such an event by the bookmaker). The GIFI has received information on this method being used for money laundering. CONCLUSION: The usage of mutual betting to legalise funds from illegal sources constitutes a high threat of money laundering.

Table no. 22

Type of services, financial products used	casino
General risk description	usage of games offered at casinos to obfuscate the origin of the cash held
Risk emergence scenario (e. g. possible example of the emergence of risk)	1. The criminal purchases chips at a casino e. g. for cash. Using a small part of them, they exchange the chips held back for money. 2. Using the game of poker, one of the criminals purposefully loses chips paid for by funds stemming from illegal sources for the benefit of a person tied to them, who then exchanges them for cash.
Vulnerability level	2

[34] https://gazetalubuska.pl/drobne-zmiany-w-kodeksie-karnym-skarbowym-to-miliardy-dla-budzetu-panstwa/ar/13900516, access 21.06.2019.

Vulnerability level substantiation	Access to gambling (in particular on-line gambling) is relatively easy. At legal facilities, however, guests are registered. Registration is a condition of guest entry to the gambling facility. It is easy to hide real identification data of a gambler on-line, but on-line payments must be made from the account of the registered person, and funds may only return to an account of a registered person. The only legal Polish *online* casino only allows poker to be played with a croupier. If the player would play at an illegal casino, it is possible to make international transactions, in particular if the accounts of the entity operating the on-line games are opened abroad. All entities offering legal 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.[35] Relatively limited information about suspicious transactions/activity is transferred by entities conducting activity in gambling (in the year 2017 this was 0.00% of all SARs from OI and 0.008% of all STRs) – as compared to other OIs. 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 ML is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of international cooperation of public administration bodies is relatively good. Existing legal provisions mostly correspond to the scope of the analysed risk.
Threat level	4
Threat level substantiation	The usage of games offered at casinos to obfuscate the source of cash held is one of the best described methods of money laundering. It is a broadly available mode, and it costs little to make use of it and is perceived by perpetrators as being very attractive. The usage of games offered at casinos to obfuscate the source of cash held does not require specialised knowledge about the casino itself or special skills with respect to the games. This method is frequently used by organised crime, and may be related to corruption of casino employees. Financial security resources used by casinos are circumvented in this *modus operandi* by way of corruption of casino employees or document falsification. The certificates of winnings issued by casinos are important documents to prove the legality of source of the funds held by criminals. CONCLUSION: The usage of games offered at casinos to obfuscate the source of cash held creates a very high threat of money laundering.

Table no. 23

Type of services, financial products used	games of chance
General risk description	purchasing winning tickets using funds stemming from illegal sources
Risk emergence scenario (e. g. possible example of the emergence of risk)	The criminal, colluding with a person operating games of chance, identifies the winners of these games. They then buy the winning tickets back from them.
Vulnerability level	2

[35] 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.

Vulnerability level substantiation	Access to games of chance is relatively easy. It is easy to hide identification data of the player, in particular if payment for the ticket is done with cash. All entities offering legal 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.[36] Relatively limited information about suspicious transactions/activity is transferred by entities conducting activity in terms of 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 case of ML is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of national 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	Purchasing winning tickets using funds stemming from illegal sources can be a method of money laundering. The GIFI has received limited information on the usage of this *modus operandi*, but this method is perceived to be of limited attractiveness. The entity making payments for games of chance or mutual bets does not provide a list of winning entities – the winners must be sought out. This method is not cheap, either, as a ten percent tax is levied on the winnings, making the costs of use higher. The use of this *modus operandi* requires planning, knowledge and skills. CONCLUSION: Purchasing winning tickets using funds stemming from illegal sources creates a medium-level threat of money laundering.

10. Area – non-profit organisations

Table no. 24

Type of services, financial products used	charity activity
General risk description	using foundations and associations for money laundering
Risk emergence scenario (e. g. possible example of the emergence of risk)	Through various straw men and shell companies, criminals transfer money from illegal activity to the benefit of the foundations and associations they control as donations. The money is then transferred to the criminals or related persons in the form of scholarships, aid, loans for business, in accordance with the bylaws of these entities.
Vulnerability level	3

[36] 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.

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 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.[37] They do not provide information about suspicious transactions/activity to the GIFI (in 2017[38] 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 ML is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of national 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 the mechanism entailing the formation of foundations and associations, through which financial resources would be transferred to selected beneficiaries, may be viewed in Poland as quite an attractive method of money laundering. Dirty money – in many methods – may be transferred to legally-operating foundations or associations, to then supply selected beneficiaries or their companies in line with the bylaws of the foundation/association using legal funds. Donors may be found among domestic or foreign entities, with which contact may be impossible should an investigation need to be carried out. The freedom to dispose of financial resources by any owner and the lack of need to explain the decisions taken about the donation made by a specific foundation improves the attractiveness of this *modus operandi*. The usage of this method does not require very specialised knowledge or unique skills from the entity legalising funds stemming from forbidden activity. CONCLUSION: The establishment of foundations or associations to transfer through them funds stemming from illegal sources constitutes a significant threat of money laundering.

11. Area – crowdsourcing

Table no. 25

Type of services, financial products used	crowdsourcing
General risk description	organising *crowdfunding* in order to legalise the financial resources held or transferred

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

[38] 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)	Organising an event entailing the collection of funds e. g. to start up a legit business via a crowdfunding platform. The funds from criminal activity are transferred by strawmen or fictitious natural persons once or in relatively small amounts.
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 ML within the scope of the analysed scenario goes undetected. The level of national 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	The organisation of a crowdfunding drive for resources can be related to certain costs (the intermediation of the crowdfunding platform is related to a commission being up to a few percent at times, usually calculated from the collected funds). In addition, it requires suitable planning and knowledge, as well as time to do it. The GIFI has no information about the possibility of usage of this method for money laundering, save for information from foreign partners (in particular contained in the supranational money laundering and financing of terrorism risk assessment drawn up in the year 2017 by the European Commission). CONCLUSION: The usage of the crowdfunding mechanism creates a medium-level threat of money laundering.

12. Area – trade in high-value goods

Table no. 26

Type of services, financial products used	precious stones and metals
General risk description	investing funds from illegal sources in the purchase of precious metals and stones
Risk emergence scenario (e. g. possible example of the emergence of risk)	1. Criminals purchase bars of gold, gold coins, diamonds and other valuable gems to transport them across the border (by courier or via postal package or cargo transport) and sell in a country characterised by less stringent control of the financial market. The money from the sale is then invested in legally operating undertakings or introduced into the banking system. 2. Criminals purchase bars of gold, gold coins, diamonds and other precious gems in other countries for the funds stemming from illegal sources that were transferred out. The purchased goods are then sold in Poland or third countries on the basis of counterfeit invoices and certificates of origin.
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 ML is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of national 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 the mechanism of investing funds from illegal sources in the purchase of precious metals and gems is one of the most frequently seen methods of money laundering. Due to the stable value of metals and gems, the simplicity of their transport (even abroad) and the relatively small volume providing the ease with which they can be hidden, this method is used relatively frequently. It is a broadly available mode, its usage costs relatively little and it is perceived by perpetrators as being rather attractive. In the substantiation attached in the year 2018 to the then-contemporary draft of the *Polish act of March 1st, 2018, on countering money laundering and financing of terrorism*, it was indicated that money laundering or financing of terrorism risk related to the operation of entities providing services in terms of trade in metals or precious and semi-precious stones primarily applies to cash transactions. Usage of the mechanism of investing funds from illegal sources in the purchase of precious metals and stones requires no highly specialised knowledge or specialised skills. This method is frequently used by organised crime, it may be related to corruption, as in certain instances it requires fake certificates or other [fake] documentation to be drawn up. The GIFI has received information on the usage of this method for money laundering. CONCLUSION: The usage of the mechanism of investing funds from illegal sources in the purchase of precious metals and stones creates a high threat of money laundering.

Table no. 27

Type of services, financial products used	antiques and works of art
General risk description	investing funds from illegal sources in the purchase of antiques and works of art
Risk emergence scenario (e. g. possible example of the emergence of risk)	Criminals purchase antiques and works of art for funds stemming from illegal sources; they store these, treating them as a kind of investment, or transport them abroad for sale.
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 ML is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of national 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 use of the mechanism of investing funds from illegal sources in the purchase of antiques and works of art is a method of money laundering. It is a long-term and profitable investment, however, one that has a few disadvantages. The main advantage of works of art is continues appreciation of value, and it is quite difficult to lose on such an investment, as demand regularly rises while supply is limited. The downside, however, is limited liquidity, and there is a very limited number of valuable objects in trade on the market. Investing in antiques and works of art requires a lot of patience, and profit depends on the current trend or fashion. One has to know the market very well and be quite experienced. Investing requires the use of advisory services, a price estimate must be made, and the authenticity of the items may be problematic. The use of the mechanism of purchasing antiques and works of art by investing funds from illegal sources is rather perceived as a money laundering method of limited attractiveness.The GIFI has received little information on the use of this method for money laundering. CONCLUSION: The use of the mechanism of investing funds from illegal sources in the purchase of antiques and works of art gives rise to a medium-level threat of money laundering.

13. Area – real property trade

Table no. 28

Type of services, financial products used	purchase/sale of real property
General risk description	investing funds from illegal sources in real estate
Risk emergence scenario (e. g. possible example of the emergence of risk)	1. Real estate purchased for legal or laundered funds at market prices by criminals is then transferred as a contribution-in-kind to a newly founded company. Its value is then exaggerated, and, accordingly, the value of the company itself also rises. Then, perpetrators sell shares in the company to a straw man who in actuality only pays the market price of the real property. 2. A property is purchased by criminals for an artificially low price for legal or laundered funds. The difference between the purchase price and the market price is paid to the seller unofficially by funds from illegal sources.
Vulnerability level	2

Vulnerability level substantiation	The purchase/sale of real estate is hindered by provisions requiring such transactions to take the form of notary deeds (art. 158 *of the Polish Civil Code*). Furthermore, the purchase of real estate in Poland by foreigners may only take place with further limitations in place (e. g. following approval by the Polish minister of internal affairs). It is difficult to hide the identification data of the buyer and seller. International transactions are possible if they apply to real estate located abroad or if the accompanying financial transactions are effected by way of accounts kept abroad. Intermediary entities in the transactions (notaries, real estate intermediaries) are OI. Real estate developers selling properties on the primary market are not OI. OI from this area do not transfer or transfer relatively little information about suspicious transactions/activity to the GIFI (in the year 2017 there were no STRs or SARs from real estate intermediaries; notaries transferred 0.0032% of all STRs, and including lawyers and legal advisors – 0.61% of all SARs from 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 case of ML is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of national 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 the mechanism entailing investing funds from illegal sources in real estate may be perceived in Poland as a quite attractive method of money laundering. Exaggerating or artificially reducing real property value in transactions conducted between related persons or enterprises and using the difference between the real/market price of the property and the invoice/contract price (this one being exaggerated) is 'profit' for the purchaser/seller in the form of legalisation of that part of the funds. The freedom of making contracts and the large number potentially differentiating the value of similar properties increases the attractiveness of this *modus operandi*. The usage of this method does not require the entity legalising funds from criminal activity to have highly specialised knowledge, perform broad planning work or have unique skills. CONCLUSION: Investing funds from illegal sources in real estate constitutes a significant threat of money laundering.

14. Area – safe deposit boxes

Table no. 29

Type of services, financial products used	Safe deposit boxes
General risk description	hiding funds from illegal sources in safe deposit boxes
Risk emergence scenario (e. g. possible example of the emergence of risk)	Perpetrators renting out numerous safe deposit boxes to store funds from illegal sources until they are introduced to the banking system. Regular introduction of small amounts of funds kept in these safe deposit boxes to the banking system.
Vulnerability level	2
Vulnerability level substantiation	Some banks provide services entailing the provision of safe deposit boxes to customers, but they are not available at all branch offices. In theory, a safe deposit box can be rented by anyone. The costs of renting a safe deposit box as compared to the costs of holding a bank account is relatively high – usually up to several hundred PLN per year. Beside banks, other businesses offer such services as well, operating on the basis of the provisions of the Polish act of *March 6th, 2018 – Entrepreneur law.* A safe deposit box only allows the storage of assets. In order to complete a transaction, the customer must use other products and services offered by banks and other financial institutions. It is difficult to hide customer data. All entities offering the products/services indicated above are OI.

	Banks use customer due diligence measures. They are characterised by good awareness of the ML/TF risk. They analyse transactions efficiently. The most 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). As for entrepreneurs pursuant to the *Polish act of March 6th, 2018 – Entrepreneur law*, conducting activity entailing the provision of safe deposit boxes, as well as branches of foreign enterprises offering such services in Poland, they are a new category of obliged institutions that is liable to adhere to obligations stemming from the provisions on countering money laundering and financing of terrorism beginning July 13th, 2018. 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 ML is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of national 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	Safe deposit boxes allow the storage of certain kinds of assets related to illegal activity, and at the same time provide the possibility of hiding them from law enforcement authorities. Some banks offer these services. It is necessary to sign a contract with the bank to use it, making all data of the depositing party available to law enforcement officials conducting a criminal investigation with respect to the tenant, or to a bailiff. One must remember, however, that criminals may also use safe deposit boxes not only made available by banks, but by specialised businesses as well. This *modus operandi* is relatively simple, it does not require complex planning. The GIFI had not received much information on hiding funds from illegal sources in safe deposit boxes, both in terms of residents as well as non-residents. CONCLUSION: Hiding funds from illegal sources in safe deposit boxes in Poland constitutes a significant threat of money laundering.

15. Area – business activity (general)

Table no. 30

Type of services, financial products used	legal business activity of entities
General risk description	usage of active business entities for money laundering
Risk emergence scenario (e. g. possible example of the emergence of risk)	1. Purposeful fusion of funds from illegal activity with legal profit of the business entity dealing in international trade, to hinder identification of the source of specific funds. 2. Usage of economic entities that for the most part profit from their business activity in cash (e. g. restaurants, hotels). The overstated total profit amount becomes the mode of introduction to legal business trade of funds stemming from illegal activity.
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 small of the entities of businesses belong among 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 ML is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of national and international cooperation of public administration bodies is relatively good. Existing legal provisions mostly correspond to the scope of the analysed risk.
Threat level	4
Threat level substantiation	The usage of operating business entities to launder money is one of the most frequently used methods of money laundering. It is a broadly available mode, and it costs little to make use of it and is perceived by perpetrators as being very attractive. The usage of operating business entities to launder money requires no specialised knowledge about the banking system or detailed, specialised skills. Frequently used by organised crime. Should an organised crime group receive funds e. g. from street drug sales, these are used for laundering the money of the business, which potentially creates their profit in cash. The low cost of the method is ensured by creative accounting and tax optimisation. The GIFI receives information about usage of this method for money laundering. CONCLUSION: The usage of operating business entities for money laundering creates a very high threat of money laundering.

Table no. 31

Type of services, financial products used	shell companies
General risk description	usage of companies, that in practice do not run business, for money laundering
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 from illegal activity. 2. Perpetrators create complex and long chains of organisational and ownership tiles among business 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 money laundering difficult. 3. Transfer of asset values between the above described titles (e. g. purchase/sale of goods and services, number of shares, provision/repayment of loans) in order to obfuscate their origin. 4. Using accounting and administrative services offered by the relevant business entity specialising in such work, in order to introduce and keep a limited-liability company utilised for money laundering.
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 partnerships – 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 ML is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of national and international cooperation of public administration bodies is relatively good. Existing legal provisions mostly correspond to the scope of the analysed risk.
Threat level	4
Threat level substantiation	The usage of companies that practically do not conduct business, for the purpose of money laundering, is one of the most frequently encountered money laundering methods. It is a broadly available mode, it costs little to make use of it, and it is perceived by perpetrators as being attractive and safe. It is frequently treated as a necessary component in operations aimed at the legalisation of funds from criminal activity. Usage of companies that practically do not conduct business does not require specialised knowledge on the banking system or special skills. In practice, one uses solely the bank accounts of such business-simulating companies. A shell company should only take the form of an intermediate component in a transaction chain aimed at the obfuscation and extension of the transaction path for the money being laundered. However, it may also take the character of a final link in a transaction chain. A shell company may be a domestic entity, but it may also be registered with a foreign jurisdiction, in particular a „tax haven', where restrictive provisions are in place with respect to bank secrecy. The GIFI receives information about this method being used for money laundering. CONCLUSION: The usage of companies that in practice do not conduct business activity creates a very high threat of money laundering.

Table no. 32

Type of services, financial products used	legal and tax advisory services
General risk description	usage of intermediation of other entities to legalise funds from criminal activity
Risk emergence scenario (e. g. possible example of the emergence of risk)	Support of criminals (often without awareness of the actual objective) in making property and high-value goods purchase transactions, in the establishment and operation of business entities, foundations and trusts as well as the execution of bank transactions by making own bank accounts available.
Vulnerability level	3

Vulnerability level substantiation	Access to legal and tax advisory services is relatively easy. They can support the hiding of customer identification data and the execution of international transactions. Entities providing such services are OI. They possess a certain awareness of their obligations in terms of AML/CTF. OI from this area do not transfer information at all or transfer relatively little information about suspicious transactions/activity to the GIFI (in the year 2017 they transferred ca. 0.034% of all STRs and ca. 0.98% of all SARs from OI[39]). 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 ML is detected spanning the analysed scenarios, and afterwards the perpetrators are indicted and punished as a result of proceedings/investigation. The level of national and international cooperation of public administration bodies is relatively good. Existing legal provisions correspond to the scope of the analysed risk to a limited extent.
Threat level	4
Threat level substantiation	The usage of intermediation of other entities (often without awareness of the actual objective) to transfer and legalise funds stemming from illegal sources is one of recognised money laundering methods. The GIFI has information about the use of this *modus operandi*. An entity providing the above-described services may provide the criminals with access to specialised legal and tax knowledge. This can substantially aid in laundering money from criminal activity. Not without significance is also the possibility of depositing financial resources in bank accounts belonging to such intermediaries, e. g. as a deposit. The payment or transfer to another account from such an account is tantamount to pretending the legal origin of asset values obtained in course of criminal activity, and bears all the hallmarks of legalising the funds being laundered. Usage of such intermediation is also significant due to the fact that such services may sometimes be necessary to execute a particular transaction. Sole access to such services is quite easy and requires no particular competences or specialised knowledge. This *modus operandi* may be perceived by perpetrators as quite an attractive and safe money laundering method. CONCLUSION: Usage of intermediation of other entities to transfer and legalise funds from illegal sources creates a very high threat of money laundering.

[39] Along with auditors and accountants.