2022

Report

REGARDING THE NATIONAL RISK ASSESSMENT ON MONEY LAUNDERING AND TERRORISM FINANCING

The National Office for the Prevention and Control of Money Laundering (FIU Romania),
The National Bank of Romania,
The Financial Supervisory Authority,
The Ministry of Justice,
The Ministry of Internal Affairs
The Prosecutor's Office attached to the High Court of Justice,
The Romanian Intelligence Service

Report developed within the project

SRSP 2020/137.01 "Money Laundering and Terrorism financing Risks Compliance: Implementation of National Mechanism to Assess and Manage Money Laundering and Terrorism Financing Risks in Romania"
Project FUNDED of commission European in the program of Support for reforms structure 2017-2020

MAIN FINDINGS AND CONCLUSIONS OF THE REPORT ON THE NATIONAL RISK ASSESSMENT ON MONEY LAUNDERING AND FINANCING OF TERRORISM FOR THE PERIOD 2018-2020

Content

I. Introduction to the National Assessment regarding the Risks of Money Laundering and Terrorism Financing

Preamble

- The performance of the National Risk Assessment regarding Money Laundering and Financing of Terrorism complies both with the criteria imposed by Recommendation 1 of the International Financial Action Task Force (FATF) and with the legal obligations imposed by Law 129/2019 on the prevention and control of money laundering and financing of terrorism, including the amends and additions of certain legal acts, as they were notified by Romania to the European Commission after the provisions of the Directive 2015/849 (AMLD4) have been turned into national rule.
- The main objective of this approach at national level is for the Romanian authorities to realistically identify the risks of money laundering and terrorist financing and to ensure that the necessary measures are taken to reduce them through the efficient allocation of financial, technical and human resources.
- The national assessment of these risks is of particular importance at the macro-economic level, because based on its outcomes, Romania will be able to improve its regime so as to prevent and combat money laundering and terrorist financing by:

◆ Getting to know the risks of money laundering and terrorist financing;
◆ Assessing the effectiveness of risk mitigation strategies;
◆ Prioritizing risk mitigation activities;
◆ Making justified decisions regarding the limitation of the coverage of low-risk sectors and products from the point of view of preventing and combating money laundering and terrorist financing;
◆ Redistributing resources to address the areas identified as priorities.

- The inter-institutional cooperation developed throughout the implementation of the present process of national assessment regarding the risks of money laundering and financing of terrorism provides grounds for the consolidation of a practice of a risk-based approach in the field, which will certainly become permanent when specific assessments will be carried out periodically.

The methodology used

- The National Office for the Prevention and Control of Money Laundering (NOPCML) together with the National Bank of Romania (NBR) and the Financial Supervisory Authority (FSA) initiated the national assessment of money laundering and terrorist financing risks in Romania in September 2019.
- In order to implement the project, a Steering Committee was established, made up of representatives of the NOPCML, NBR, FSA, POHCCJ, MJ, MIA and RIS. The members of the Steering Committee contributed in taking the most important decisions in accordance with the Assessment Methodology provided by the Council of Europe.
- According to the Methodology, the data collected and used refers to the period 2018-2020, the information regarding the cases of convictions and referrals to court for the crime of money laundering/terrorist financing constituted the starting point for the macroeconomic analysis that is the subject of this report. The statistical data related to the analyzed sectors, available to the supervisory authorities, was also added.
- At the same time, the data and information regarding ongoing investigations into money laundering were collected based on a questionnaire from prosecutors from all

the competent units in the country (including the specialized bodies NAD and DIOCT).

- Other categories of information that were the basis of the risk analysis refer to the perceptions of the actors involved, obtained by completing questionnaires and participating in focus groups, as well as to information from external sources such as the Supranational Risk Assessment carried out by the European Commission or the documentary materials of the GAFI/FATF and other relevant international organizations.
- The national assessment of money laundering and terrorist financing risks was thus based on a comprehensive analysis of the following components:
    - analysis of the threats arising from predicate crimes which are the main source for the generation of criminal income subject to recycling;
    - analysis of subjects who undertake money laundering activities;
    - analysis of economic sectors with a significant risk of money laundering;
    - analysis of financial sectors and products that can be used abusively for money laundering and terrorist financing;
    - the cross-border characteristics of money laundering;
    - analysis of terrorist financing risks.
- According to the used Methodology, the level of risk assigned to each sector/product/channel/subject is based on the probability of money laundering/terrorist financing and their consequences, generating a risk determined by means of the risk assessment and the risk matrix. **The assessment of the likelihood** is assimilated to the assessment of the frequency with which criminals can undertake money laundering actions, taking into account their knowledge and skills in this regard (typologies and case studies playing an essential role) and the impact of preventive and recovery controls. **The assessment of consequences** is related to the assessment of the volume at which criminals can launder money.
- In relation to the risk matrix following the integration of the assessment of the probability and the estimated consequences, the assigned risk level can be low, medium, high and extreme.

Brief presentation of the Report's findings

Predicate crimes generating criminal income

- **Tax evasion** represents a relevant source generating criminal income that is suitable to be recycled so that, taking into account the significant damages highlighted and the conclusive statistical data in the Report, it is appreciated that the risks associated with the laundering of money from tax evasion are high.
- **Corruption** represents a criminal phenomenon with a **high impact** from the perspective of money laundering risks, considering the frequency and the large volume of the criminal proceeds found in the cases investigated and those finally resolved, but also the subjective perception expressed in the majority of processed questionnaires.
- The analysis carried out reveals that **human trafficking** allows money laundering through the use of cash, the use of middlemen and carriers, so the money laundering risks associated with human trafficking are high.
- **Computer crimes** are usually committed by Romanian citizens abroad and the criminal proceeds were transferred through money carriers in Romania; the upward trend observed in recent years at the level of the authorities that implement such cases, justifies the assessment of these risks as high.

- Based on existing data and national judicial practice, it is estimated that the phenomenon of smuggling, especially cigarettes, presents an average risk of money laundering.
- The risks posed by drug trafficking for money laundering (predicate crimes are committed abroad by organized crime groups, and Romania is a transit point for the transfer of narcotics to other countries) can be assessed as medium.
- Although crimes against the environment (illegal deforestation, waste management) did not have a major impact in the analyzed period, currently it was found that these crimes are gaining consistency, being linked to an exposure to the risks of money laundering as it results from the existing data regarding the organized crime groups that operate especially in Bucharest and its proximity, as well as the large sums of money from uncertain sources transferred through the bank accounts of front companies (with the object of waste management activity).

Risks of money laundering

Relative to the subject submitted to the money laundering risk analysis

- **Resident legal entities** from Romania present an average risk, as Romanian companies can be used to carry out illicit activities, including money laundering. Taking into account the criminal case law, the report highlights a number of examples where resident companies are involved in money laundering activities, especially illegal money derived from tax evasion (the most common predicate crime encountered).
- **Resident natural persons** are exposed to an average risk, an aspect that derives mainly from the use of personal accounts belonging to natural persons with the aim of dissimulating commercial activities specific to legal persons. Mitigation of this risk is achieved through the use of bank accounts for carrying out commercial activities, provided that the procedure applied for opening a bank account involves the application of KYC (know-your-customer) measures which significantly reduce exposure to risk.
- **Publicly exposed persons** present a high risk, especially in terms of the position held, which allows them to have access to public funds and to be protected to a certain extent by their investment in such a position, and this status creates an important advantage that might be used by the money launderers. This conclusion is also supported by the results of the analysis of predicate crimes, which revealed a high risk in relation to corruption crimes.
- **Non-resident natural persons** pose a low risk given that they represent a low percentage of people convicted under the Law on the prevention and control of money laundering and financing of terrorism.

Relative to the economic sector that is subject to money laundering risk analysis

- **The real estate sector** (including construction - trade in construction materials, developers and real estate agents) represents a real challenge from the point of view of combating money laundering, being characterized by a high degree of risk, given the number of convictions in this sector, as well as the amount of money laundered. This perspective also took into account the widespread use of cash in the real estate sector, especially for the purchase of construction materials and for the payment of workers, who are largely outside the labor market.
- **The agricultural sector** presents a medium risk, being exposed in particular due to the use of cash and the possibility of accessing subsidies from the EU budget or the

national budget, fictitiously and which are used for purposes other than those for which they were granted. In addition, awareness of the risk of money laundering through the sector is limited.

- **The oil and natural gas trading sector** has an average risk, in the context in which the most common predicate crime was tax evasion, and organized criminal groups could use the sector to hide the illicit origin of money, as a result of the fact that the commercial operations carried out in this sector involve large amounts of money.
- **The trade sector** presents an average risk as a result of the fact that most companies or authorized natural persons are registered in the national trade register and have bank accounts, in both cases the commercial entities are under the supervision of the competent authorities. Moreover, the vast majority of commercial operations intersect at a given moment with the banking system, being seconded by the performance of financial-banking operations, which leads us to apply the rules of knowing the clientele within financial institutions, these operations falling under the scope of supervision performed by them. Companies also interact with other categories of reporting entities (accountants, auditors, notaries, lawyers, consultancy firms, etc.), each of them applying its own set of know-your-customer measures and monitors, in accordance with the law, the entire business relationship with that company.

Relative to the category of reporting entities that are subject to specific legislation from the perspective of the analysis of exposure to the risk of money laundering

- **The banking sector** presents an **average residual risk**[1], partly due to a more mature control environment compared to the rest of the obliged entities. However, the high volume of turnover and the natural focus of the sector on the management and transfer of assets means that the banking sector as a whole is normally exposed to the risk of money laundering.
- **Electronic money issuing institutions subsector** following on-site inspections, it was assessed as being exposed to a medium-high residual risk.
- When assessing the residual risk associated with the activity of financial instruments intermediaries, respectively when assessing the risks after the application of mitigation measures, it was found that financial instruments intermediaries present an average residual risk of being used for the purpose of money laundering
- When assessing the residual risk associated with the activity of delegated agents[2], respectively when assessing the risks after the application of mitigation measures, it was found that the investment agents/delegates present an average residual risk of being used for the purpose of money laundering.
- When assessing the residual risk associated with the management of collective investment funds (open-end and closed-end investment funds), respectively when assessing the risks after the application of mitigation measures, it was found that investment fund management companies present an average risk residual to be used for the purpose of money laundering.

[1]**Residual risk** - the risk regarding the fulfillment of the objectives, which remains after the establishment and implementation of the response to the risk

[2]**Delegated agent** - natural or legal person who, under the full and unconditional responsibility of a single financial investment services company on whose behalf he acts, based on a contract, promotes investment services and/or related services to clients or potential clients, receives and transmits instructions or orders from clients regarding financial instruments or investment services, place financial instruments and/or provide clients or potential Clients with consulting services regarding these instruments or services.

- When assessing the residual risk associated with the activity of a credit institution authorized as a depository or custodian of securities, respectively when assessing the risks after the application of mitigation measures, it was found that depositories of financial instruments present an average residual risk of being used for laundering purposes of money.
- It is estimated that relative to the identified risk, vulnerabilities, threats and remedial measures and preventive response measures, insurance companies and insurance intermediaries present an average risk of being used for money laundering purposes.
- When assessing the risk associated with the activity of administering voluntary pension funds, it was found that non-bank financial institutions, respectively administrators of voluntary pension funds, especially due to the characteristics of the managed product, present a low risk of being used for money laundering purposes.
- The sector of non-bank financial institutions (NBFIs - registered exclusively in the General Register of the National Bank of Romania and which do not have the status of payment institution or electronic money institution), supervised by NOPCML presents a medium risk, as it is considered that money laundering through NBFIs could be possible by criminals or their intermediaries obtaining loans to be repaid using illicit funds, even if the related costs are higher than in the case of other offers on the market, in order to benefit from the fact that the application of know-your-customer measures may in some cases be less rigorous than in banks.
- **The sector of pawnshops** (non-banking financial institutions registered in the National Bank of Romania's Register), supervised by NOPCML, present a medium risk, taking into account the fact that in their case the frequent use of cash is identified and the fact that there are difficulties in terms of identifying the real beneficiary of the clients as well as in relation to the determination of the origin of the funds / goods involved in the transactions.
- **The sector of mutual aid societies** (non-bank financial institutions registered with the National Bank of Romania), supervised by NOPCML, presents a low risk in terms of money laundering threat.
- **The sector of currency exchange houses** presents a medium risk, taking into account the fact that amounts from criminal sources can easily be subjected to successive currency exchanges, in various currencies, in order to facilitate the running of complex operations aimed at disguising the real origin of the assets involved.
- In terms of money laundering risk exposure of the gaming provider sector:
    a) **Casinos (land-based or online) and online gambling** poses a high risk, given that the sector is attractive for laundering the proceeds of crime, which requires a medium level of expertise, as illegal proceeds can easily be converted into legitimate gambling winnings.
    b) On the other hand, for betting (land-based) gambling service providers and (land-based) slot machines, given the majority use of cash, the possibility of easily disguising the identity of the real beneficiaries, but also the relatively small amounts played, it is estimated that the risk level is average.
- Professionals such as lawyers and notaries public are exposed to a medium level of risk, given the advisory services they can provide to potential offenders in setting up complex corporate structures for the investment and transfer of illicit funds. Professionals such as chartered accountants and accounting experts as well as tax consultants are also exposed to a medium level of risk as the services they provide may be attractive to criminals as they could facilitate the creation of an appearance of legitimacy for funds of illicit origin. Equally, these professionals are attractive to

criminals because, through their professional reputation, they provide an appearance of legality and good repute which they can use to deceive the vigilance of reporting entities. However, it is worth noting the quality of the oversight work in these cases by professional self-regulatory bodies, as their contribution to increasing compliance and due diligence is obvious.

- Other professionals such as auditors and appraisers present a low risk, considering the way in which they carry out their activity and the type of services offered which are factors that reduce the level of vulnerability. Also, the analysis found an intensive surveillance activity of these entities, which contributes favorably to mitigating the identified risks.
- The money laundering threat related to other legal professionals is considered medium for insolvency practitioners and low for bailiffs.
- Considering that in Romania real estate agencies do not have specific regulations and are not coordinated by a self-regulatory body and the degree of awareness of the sector regarding the risks of money laundering still seems to be limited, taking into account the fact that the enforcement institutions of the law have identified cases in which the money obtained from crimes was laundered through real estate investments, and other activities of supervision of the sector have revealed non-compliance with the legal provisions, it is estimated that the risk exposure for real estate agents is high. **Services provided by management and business consulting professionals,** regarding including financial or accounting aspects, can be frequently used in money laundering schemes and are considered by criminals to be the best way to compensate for their lack of expertise, these elements thus arguing for the consideration of the fact that the level of money laundering threat related of the services provided by professionals providing managerial and business consultancy is to be considered high.
- **Service providers for companies or trusts**, other than those provided for in letters (e) and (f) of Law no. 129/2019, presents a high risk considering the fact that they often offer services that can facilitate the creation of legal constructions/companies with complex, opaque structures, attractive to people who intend to initiate transactions in which they use the money from crimes, for make it impossible or extremely difficult to establish a link between the funds and their illicit origin.
- As far as art dealers are concerned, the analysis reveals a medium risk of exposure, given that the art trade is an attractive sector for money laundering, requiring a high level of expertise and more elaborate training than in other sectors and the art trade, artefacts and antiques is largely carried out through private transactions, as the persons involved in such transactions do not have a self-regulatory body nor a structured general knowledge of anti-money laundering and anti-terrorist financing legislation (as revealed by the analysis of the sample of questionnaires completed by entities in the sector).
- In recent times, cryptocurrencies and virtual currency have been highly developed and they are an emerging sector, leading to the assessment that providers of such virtual assets are high risk. In this context, the interest shown by organized crime groups is growing, especially as there is weak institutional control and the sector is characterized by the anonymity of transactions, speed and no limits on the volume of funds transferred.

Cross-border characteristics of money laundering and terrorist financing

- Cross-border risk is classified as high because collecting data on the origin of money that has been transferred to Romania is a lengthy and costly process, and most of the time money of uncertain origin only transits accounts opened in Romania.
- From a money laundering point of view, the globalization process allows money to be easily transferred to different regions of the world, which increases the possibility of using such operations to hide funds of illicit origin. In addition, criminal networks operate in more than one country to reduce the chances of detection, the use of multiple jurisdictions (including offshore jurisdictions) limits/reduces the efforts of authorities to uncover the perpetrators of crime.
- The risk of terrorist financing through cross-border transfers is low because the money is usually transferred to Romania through financial institutions that apply know-your-customer measures, either remaining in Romania or being transferred abroad and thus permanently under banking control, and this channel is avoided by terrorists.

Terrorist and terrorist financing risks

- So far, no networks have been identified on the territory of Romania operating for the purpose of obtaining, collecting or transferring funds for the benefit of terrorist organizations/entities/groups.
- There have been occasional cases where foreign residents have transferred various amounts of money to conflict zones, without it being possible to determine with certainty the real beneficiaries of the funds, the motivation (strictly personal or support for a terrorist entity) or how the funds were used. The movements were not directed or ordered by terrorist organizations and were sporadic, individual and unorganized.
- In the case of the 8 persons convicted of involvement in terrorist offences, including the person convicted of involvement in terrorist financing activities, checks were carried out on the source of the funds. The checks revealed that no considerable financial effort was required to commit the offences and that the funds came from own sources.
- The international climate for terrorism, persons/entities issuing/distributing and/or trading any form of electronic money/virtual assets, money remittances through money transfer service providers with an extensive network of global agents, including hawala and other informal money and value transfer systems, are considered/approached by the authorities as risk elements in relation to terrorist financing, even if they have not manifested themselves in Romania.
- As the prevention of terrorist financing activities remains a priority at institutional level and within the NTPFTS, the authorities in charge of the field have permanently adopted a preventive-anticipative approach in the management of suspicious situations, constantly monitoring and assessing the level of risk generated by persons suspected of being involved in terrorist financing activities.
- On the basis of these assessments, the cases of terrorist financing presented in the National Assessment Report have been identified and documented, and in some cases the need to put in place preventive measures has arisen, including the declaration as an undesirable person or the prohibition to entry Romania.
- In the area of preventing and combating terrorism (including financing activities), inter-institutional and international information exchange is constantly being considered. The mechanisms already in place in this respect allow for an appropriate level of cooperation, and it is appropriate to facilitate rapid and secure cross-border access to financial data to allow early detection of operations.

- The risk of terrorist financing in Romania can therefore be assessed as Low.

Findings of the National Money Laundering and Terrorist Financing Risk Assessment

- Money laundering is a complex process, the seriousness of which is by no means negligible, especially in the context of financial instability, imbalances and vulnerabilities of the economic system, generated by the crisis period, during which the risk of such criminal phenomena increases significantly.

Thus, in times of crisis, money laundering and organized crime can be observed to increase, often linked to specific activities of the underground economy due to fiscal pressure, increased corruption and other similar phenomena.

- As a general note, this report notes that the intensive use of cash leads to a high risk of its use by organized crime groups to hide the illicit origin of money. The cases analyzed in this report have shown that, at national level, extensive use of cash is the main method of money laundering. In addition, there are many economic sectors in Romania that allow intensive use of cash transactions, such as construction, real estate development, agriculture, waste industry, exchange houses, gambling.
- Beyond these general findings, it should be pointed out that Romania is a country with a relatively limited attractiveness for money laundering, due to specific regulations and a relatively low degree of financial secrecy, all of which are addressed and analyzed in the context of the corresponding weight of the national economy in the overall regional and global economy.
- In Romania, the financing of terrorism remains at a very low level and is cyclical, depending on developments abroad. Our country does not face an indigenous terrorist phenomenon and there are no terrorist organizations or cells operating on our national territory. Moreover, no networks have been identified on our national territory with the purpose of obtaining, collecting or transmitting funds abroad for the benefit of terrorist organizations or persons involved in activities qualified as terrorist acts. The measures taken so far have helped maintain the national security environment and have prevented terrorist threats from materializing.
- It was found that there are areas of defficient legislation that may favor the materialization of some of the risks identified, such as, in the vast majority of cases, an inadequacy of the resources available to the competent authorities was also indicated, particularly of the recent IT tools and technologies that would allow adequate responses to current social realities.
- Another general factor increasing the risks is the insufficient awareness of the reporting entities of the criminal phenomenon to which they are exposed, as well as a low public awareness regarding the importance of preventing and combating money laundering and terrorist financing, which makes them reluctant to cooperate with the competent public authorities.
- Looking at the sectors concerned as a whole and at the types of actors involved in the process, the report concludes that the national institutions responsible for controlling money laundering and terrorist financing have the capacity to identify and combat effectively all the activities of an illicit nature that generate dirty money and the risk of money laundering and terrorist financing.
- The findings contained in this Report on the National Assessment of Money Laundering and Terrorist Financing Risks must be viewed and analyzed in their dynamics, with reference to the economic dimension of each sector under analysis, but also to the elements of content that typically define money laundering and terrorist financing risks.

II. Money Laundering and Terrorist Financing Risk Assessment by Topic

During the period under review, the number of resident legal persons convicted for money laundering was quite small, namely one case of money laundering with the predicate offence of tax evasion (the amount laundered being EUR 12 million in the petroleum products trade sector) and one case where the predicate offence was bribery (the amount laundered being EUR 40,000).

Non-resident legal persons were convicted in two money laundering cases. In one case the predicate offence was embezzlement, the amount laundered was €4,000,000, and in the second case the predicate offence was theft, the amount laundered was €176,000.

Resident individuals *were involved in 116 money laundering convictions. The main predicate offences committed in these cases were tax evasion, fraud, embezzlement, abuse of office, forgery and trafficking in human beings*.

The number of non-resident individuals who were convicted of money laundering offences was the subject of 7 cases. The main predicate offences involving non-resident individuals were abuse of office, tax evasion, fraud and embezzlement. The main method used by the perpetrators was the reconstitution of land ownership through false ownership documents.

Resident publicly exposed persons *were convicted in 6 cases of money laundering and the predicate offences were: trading in influence, tax evasion, bribery and abuse of office*.

The main subject of money laundering convictions is resident individuals and accounts for 74.80% of the total number of convictions.

Non-resident individuals account for 5.30% of all convictions analyzed in this report, as previously mentioned in this chapter.

Legal persons

According to data available at the National Bank of Romania, the number of resident legal persons who are clients (with resident beneficial owners) in the banks' portfolios is of 1,271,741, representing 91.95% of the total number of legal entity clients. The number of resident legal entity clients (with at least one non-resident beneficial owner) in banks' portfolios is 107,658, representing 7.78% of the total number of legal entity clients. The number of non-resident legal entity clients in banks' portfolios was 3,739, representing 0.27% of the total number of legal entity clients.

This report has taken into account the ML/TF risks to which legal persons established under Law 31/1990 on companies (legal persons carrying out profitable activities), republished, as subsequently amended, and GEO 26/2000 on foundations and associations (non-profit persons).

As per the provisions of the Law 31/1990, companies may have one of the following statutory forms:

General partnership;

- Limited partnership;
- Joint stock company;
- Limited partnership limited by shares; and

- Limited liability company.

The situation of the entities registered in the National Trade Register was as follows:

Structure	2018	2019	2020
SRL	915,581	973,182	1,024,889
TO	6,576	6,436	6,332
PFA	247,472	236,638	248,154
SCS	129	126	120
CNS	1,701	1,614	1,559
SCA	0	0	1
TOTAL	**1,171,459**	**1,217,996**	**1,281,055**

Law no. 129/2019 is the legal instrument transposing into national law the provisions of the 4th AML Directive, and Article 56 establishes the obligation for legal persons subject to the obligation of registration in the National Trade Register and the obligation to declare the beneficial owner.

In Romania there are three registers of beneficial owners, as follows:

(a) the register organized at NTRO (National Trade Register Office) level for legal entities obliged to register in the Trade Register, with the exception of autonomous companies[3], of national societies[4] and of companies fully or majority owned by the Romanian state; (b) the register organized at the level of the Ministry of Justice (MJ) for associations and foundations; (b) the register organized at NAFA (National Agency for Fiscal Administration) - Ministry of Finance (MF) level for trusts.

According to the centralized evidence regarding convictions, legal entities were used by resident and non-resident natural persons in order to launder sums of money obtained from crimes, as follows:

- tax evasion;
- deception;
- embezzlement.

The main way used in money laundering cases involving companies is internal transfers through company bank accounts followed by cash withdrawals.

The NBR data showed that cash deposits made to the accounts of legal entities (especially highly liquid activities) in 2019 amounted to €103,604.0926 million and €50,996.4459 million in 2020. The situation regarding cash transactions should be analyzed within the context of the Covid-19 pandemic which through the imposed health restrictions caused the contraction of the national economy and the total volume of cash receipts. Taking all these arguments into account, the volume of cash used at the level of legal entities is still high in the Romanian economy.

[3]The autonomous authority is organized and operates in the strategic branches of the national economy - the arms industry, energy, mining and natural gas, postal and railway transport - as well as in certain areas belonging to other branches established by the government, currently the exception is eliminated by GEO no. 123/2022;

[4]National companies are organized as commercial companies by decision of the Government, and those of local interest by decision of the local state administration body.

The widespread use of cash creates a vulnerability from a money laundering point of view. This vulnerability is also mentioned in the Supranational Risk Assessment on Money Laundering and Terrorist Financing in the European Union (NARS). In this context, it is important to strengthen financial discipline measures on cash receipts and payments.

Associations and foundations

Natural and legal persons carrying out general interest activities or act in the interest of the community or, where appropriate, in their personal interest, may form associations or foundations - private legal persons with no property purpose - under the terms of the law (political parties, trade unions and religious cults are not covered by this Law). Two or more associations or foundations may form a federation. Associations, foundations and federations may carry out any other direct economic activities if they are ancillary and closely related to the main purpose of the legal person. Associations, foundations and federations may be shareholders in companies.

An association, foundation or federation may be recognized by the Romanian Government as being of public utility (activity carried out in areas of general public interest or in certain communities) if several conditions laid down by law are met. Associations or foundations of public utility are recognized by Government Decision, at the request of the association or foundation in question.

The Ministry of Finance, through the Economic and Financial Inspection Department, shall control the justification, granting and justification of the sums received from the general consolidated State budget.

Associations and foundations must keep records of all their transactions for at least 5 years.

Upon establishment, annually or whenever there is a change in the identification data of the beneficial owner, the association or foundation is obliged to communicate the identification data of the beneficial owner to the Ministry of Justice for the purpose of registering/updating the record of the beneficial owners of associations and foundations.

From the National Register of NGOs - Index of Non-profit Legal Entities it results that in October 2021 a total of 126,913 entities were registered, of which: associations represent 82% of all registered entities (104,288 entities), foundations represent 16% of the total (20,268 entities), federations represent 1% of the total (1,528 entities), and the difference is represented by unions (78 entities), foreign legal entities (36 entities) and unspecified (4 entities).

Of the 104,288 associations registered in the National Register of NGOs, 98,935 are active. The main areas in which they are registered are Bucharest (17.7%), Cluj county (5.9%) and Timiș county (4.3%).

Of the 20,268 foundations registered in the National Register of NGOs, 19,139 are active. The main areas in which they are registered are Bucharest (16.7%), Suceava county (9.2%) and Cluj county (7.5%).

According to the NOPCML case analysis module, associations and foundations have not been identified as a sector in their own right in terms of reporting obligations. We note that according to Law No 129/2019, associations and foundations are not reporting entities. Prior to the entry into force of Law No 129/2019, associations and foundations were reporting

entities and were subject to the obligations set out in the Law regarding the Prevention and Control of Money Laundering and Terrorist Financing. Thus, they were obliged to establish internal supervisory controls, including know-your-customer (KYC), record-keeping and reporting measures.

With regard to the results of the off-site supervisory activity (analytical process comprising a risk assessment matrix revealing the degree of exposure to the risk of money laundering and terrorist financing of the reporting entity) carried out during the reference period by the NOPCML in relation to the "associations and foundations" sector, we mention the following:

A total of 8,979 associations were supervised off-site, with 2.9% of associations classified as high risk and 1.3% of associations classified as partially high risk.

A total of 1,535 foundations were supervised off-site, with 3.7% of foundations classified as high risk and 1.1% of foundations classified as partially high risk;
In the framework of the on-site supervision activity (on-site controls), carried out during the reference period by the NOPCML in relation to the "associations and foundations" sector, non-compliance with the legal provisions in the field was identified, regarding: internal policies, rules and procedures to combat money laundering and terrorist financing, the application of measures to know the real clientele/beneficiaries by means of risk-based circumstances, as well as the implementation of international sanctions, with the following contraventions being applied:

In the framework of on-site supervision activity carried out on a total of 130 associations, 111 contravention sanctions were applied (representing 10 fines amounting to 152.000 RON and 101 warnings).

In the framework of the on-site supervision of a total of 98 foundations, 59 fines were imposed (representing 10 fines of RON 155,000 and 49 warnings).

Conclusions - As a result of the supervision and control activities, we consider that associations and foundations may be more vulnerable to the risk of money laundering or terrorist financing due to the low level of knowledge and implementation of measures to prevent money laundering and terrorist financing, in particular with regard to the application of risk-sensitive KYC measures and the lack of awareness of the risks to which they could be exposed of being used in illicit money laundering/terrorist financing activities, especially given the (current) legal framework which does not include this type of entities in the category of AML-reporting entities.

In substantiating the above conclusions, the following aspects are taken into account: the legal framework and the control of the activity of non-profit organizations in accordance with FATF Recommendation No. 8 (transparency regarding donors) are insufficient; lack of legal instruments necessary to verify their income/expenditure; weak policies to combat misappropriation as regards NGOs, such as a statement of principles and definition of terms, strict procedures to prevent misappropriation: standardization and maintenance of bank records; standardization of accounting practices, such as account codes and donor codes; classification of costs, e.g. as direct or indirect; ensuring internal controls, including segregation of duties between staff responsible for procurement, funding, cash disbursements, salaries and liquidations; and financial reporting requirements.

There is also a lack of adequate guidance and awareness on funding indicators for non-profit organizations.

The authorities responsible for preventing and combating the financing of terrorism constantly carry out checks on situations or sources that could pose a terrorist risk and which include suspicious activities financing terrorist entities, whether they are organizations or individuals. So far, no non-profit organizations involved in financing terrorist activities have been identified in Romania.

NGOs are vulnerable because it is possible for third parties to use them to receive funds, anonymous donations, loans and online fundraising which could facilitate money laundering in the non-profit sector.

Anonymous donations are also a vulnerability in this sector. Donations can be exploited for money laundering purposes if NGOs receive donations from suspicious sources or if donors ask for the funds to be returned. Criminals could also launder funds if NGOs accept a cash loan, then return the loan to the criminal later in the form of a bank transfer.

Thus, there is a risk that high-risk individuals, such as publicly exposed persons, may make direct donations if the source of their funds is unknown or through third parties making payments on their behalf. (For example, a number of suspicious donations to pay for services such as independent tuition fees - funds that have passed through several businesses before being used to pay private tuition fees - the school in question is not immediately aware that there is any concern about the ultimate source of these funds).

General risks of products/services offered in the NGO sector

Charities often collaborate with partner organizations in different jurisdictions or with individual agents, including international transfers of funds that can be misused by individuals claiming to be associated with charities, although the risk of this happening is still low. The work of humanitarian NGOs can sometimes take place in high-risk areas where non-state armed groups or terrorists are present. However, specific risks depend on various factors, such as the level of professionalism of an NGO and the situation in the country, including the political dynamics of the conflict in question.

General vulnerability of the NGO sector to the risk of money laundering/terrorist financing and specific products

As mentioned above, some NGOs may be at risk of money laundering and terrorist financing through the use of small amounts of cash, making it difficult for law enforcement agencies and financial intelligence units to track sources of funds and transfers sent abroad using cash.

Some activities of non-profit organizations may involve higher risk in terms of funding sources (unknown/high number/international sources/high risk countries), types of activities or beneficiaries (unknown/high risk countries/high risk clients/use of channels to send money cross-border). Risks increase when formal banking channels are not available for money transfers to and from NGOs.

The non-profit sector could abuse new technological tools such as participatory finance and blockchain systems and regulators may need to assess and address any associated risks. Instead, these new tools could also be used to increase the traceability of funds.

The analysis of legal entities registered in Romania has revealed the following:

Threats:
Use of legal persons by criminals to hide the illicit origin of money.

Vulnerabilities

- Possibility of using cash to finance businesses and lack of rigorous control of the origin of the money deposited by individuals;
- Lawyers may set up companies which could then be used to hide the illicit origin of the money; registered office established at the address of the law firm (problems with searches due to professional confidentiality);
- The possibility to use the accounts of legal entities, even if they have suspended their activities;
- Lack of a legal procedure for publishing the suspension of activity in real time to prevent the use of legal entities for money laundering purposes;
- The possibility to use the company only for the transit of illegally obtained money;
- The possibility to create complex legal structures allowing the concealment of the real beneficiary and the disguising of the illicit origin of the money is an attractive point for organized crime groups;
- The possibility to exploit the procedure for setting up legal entities in Romania, which is accessible and low-cost;
- The possibility for foreign nationals to set up legal persons by power of attorney, a procedure which can facilitate the anonymity of the beneficial owner;
- limited liability companies (SRL) are particularly vulnerable to abuse, including single-member LLCs, which is the simplest form of organization that could be used.

No.	Elements	Likelihood Rating (L)	Assessment of consequences (C)	Risk rating
	The risk of resident legal entities	**Average**	**Moderate**	**Average**
Associated vulnerabilities: **Use of cash;** **Using the accounts of the resident legal entity to transfer sums of money;** **The establishment procedure is easy to access and low cost.**				
Associated threat: **Money laundering resulting from tax evasion**				
Event description: **Using the bank accounts to hide the proceeds of crime;** **Cash withdrawal to return the money to the actual beneficiary.**				
Risk description: ***It is a medium risk*** ***Average probability*** ***The consequences are moderate***				

Conclusion

Individuals residing in Romania have a medium risk of their accounts being used for money laundering purposes. Romanian companies can be used for illicit activities, including money laundering. From the case studies analyzed in this report it has been found that the accounts opened by the companies have been used to launder the proceeds of tax evasion.

As regards the risk of terrorist financing through Romanian companies, we conclude that it is low. This risk is also kept at a low level by the application by financial institutions of know-your-customer measures and controls carried out by supervisory authorities.

Natural persons (residents)

According to the NBR, the total number of current accounts held by individuals at the end of 2020 was 24,681,152 (irrespective of the number of accounts held by each customer and their currency), while the number of resident individual customers in banks' portfolios amounted to 19,580,567[5], representing 98.95% of the total number of individual customers.

In the commercial activity carried out on the domestic market, cash is used as a frequent instrument by individuals.

Regarding the volume of cash withdrawals made by individuals: in 2019 it was EUR 46,422,427,906 and in 2020 it was EUR 43,735,500,126. When comparing the volume of cash withdrawals made by individuals in 2020 with the cash deposits mentioned for legal entities, the two figures are almost similar, which raises a concern about the level of cash usage in the Romanian financial system.

On the NOPCML website one can find a Guide on suspicious indicators and money laundering typologies from which the following indicators have been listed below:

- Large cash withdrawals by a natural person;
- Inconsistency between the declared occupation of the beneficiaries of the funds and the transactions carried out through their accounts;
- Multiple cash withdrawals via authorized persons on the accounts of external cash receivers;
- Use of individuals' accounts for transactions involving commercial activities;
- Use of account proxies to carry out transactions on the accounts of third-party individuals;
- Use of individual accounts as transit accounts.

The vast majority of unbanked individuals have a poor economic education or live in an area where the banking infrastructure is not developed (mostly in rural areas), with poor education generating insufficient income for a decent living. These people may be used by criminals in money laundering flows, especially for the use of cash, without being aware of the legal consequences of their actions.
People with a low level of education and a limited income can be used by money launderers in particular by opening bank accounts in their name, and the real beneficiaries of the funds

[5] The figure refers to the number of accounts opened by individuals (some individuals may have more than one account in lei and different currencies).

channeled through these accounts may be criminals. Poorly educated people are used in this way, as intermediaries, without incurring the high cost of recycling the money.

Threats:

The use of individuals (especially low-income individuals with low levels of economic education) by perpetrators to hide the illicit origin of money.

Vulnerabilities:

- the use of individuals' accounts for the transit of proceeds of crime;
- the use of accounts belonging to individuals for cash withdrawals.

No.	Elements	Likelihood Rating (L)	Assessment of consequences (C)	Risk rating
	The risk of resident legal entities	**Average**	**Moderate**	**Average**
Associated vulnerabilities: **Use of cash;** **Using the accounts of a resident natural person to withdraw money.**				
Associated threat: **Laundering of money derived from the crime of tax evasion.**				
Event description: **Use of an interposed natural person;** **Cash withdrawals to be made available to the real beneficiary.**				
Risk description: ***It is a medium risk*** ***Average probability*** ***The consequences are moderate***				

Conclusion

Resident individuals are exposed to a medium risk because they mostly use bank accounts and the procedure for opening a bank account meets the KYC standards. Also, for cash deposits to any account opened with a Romanian bank, the individual must complete documentation on the origin of the money and the beneficial owner. A cash control system is in place in Romania, which includes on the one hand a legal limit on the use of cash and on the other hand the reporting of cash transactions exceeding the legal limit, which allows for a monitoring of cash transactions.

The risk of terrorist financing using resident individuals is low. This risk is also kept low by the application by financial institutions of know-your-customer measures and supervisory controls.

Publicly Exposed Persons (PEP)

In Romania, the list of important public functions is drawn up on the basis of Law no. 129/2019 and is published on the NIA website[6]. The Romanian legislation provides for a list containing internal and external key public functions, the actual identification of PEPs at the level of reporting entities is difficult, as the list contains only the names of key public functions, and the identification of possible associates/appropriates of a PEP is even more difficult. This problem, the identification of PEPs, was raised several times by reporting entities in the Focus Groups[7].

The identification of PEPs is not only a challenge at national level, the same challenges are highlighted at international level.

According to NBR statistics, out of the total number of PEP customers of Romanian banks (21,674 bank accounts) 95.94% are resident PEPs. Of the 4.06% of total non-resident PEP customers, only 6.57% are non-residents from high-risk jurisdictions (as determined by the European Commission). Half of the total non-resident PEP customers are from other high-risk jurisdictions and 37.71% are EU/EEA PEPs.

At the end of 2020, the volume of international transactions in resident PEP accounts was €2,904.364 million and the volume of international transactions in non-resident PEP accounts was €4,895.738 million.

During the period under review resident PEPs were subject to six convictions for money laundering, where the predicate offences were market manipulation, tax evasion, bribery and abuse of office.

Given the importance of campaign financing, it is necessary to assess the risk of money laundering in this sector.

Law 334 on the financing of political parties and elections was adopted in 2006. In 2018, methodological regulations on the application of this law were issued, updated with all new regulations in force in the EU and recommendations made by GRECO.

Threats:

Criminally funded PEPs can be used to facilitate the money laundering process.

Vulnerabilities:

- Use of donation whose source is unknown (in the case of political parties);
- Defficient application of the control mechanism of the financing activities of a political party;
- Defficient controls performed in the field of PEP integrity;
- Defficient training of civil servants in the field of public procurement.

No.	Elements	Likelihood Rating (L)	Assessment of consequences (C)	Risk rating of

[6] https://www.integritate.eu/Files/Files/Lista_functii/00%20LISTA%20FUNC%C8%9AIILOR%20PUBLICE%20IMPORTANTE.PDF

[7] Consultation groups with reporting entities, supervisory and self-regulatory bodies organized according to the methodology applied in this report.

	The risk of PEPs	**Average**	**Major**	**Picked up**
Associated vulnerabilities: **Difficult identification of PEP, especially close people;** **The use in financial transactions of persons close to the PEP;**				
Associated threat: **Crimes of corruption and similar crimes;**				
Event description: **Use of PEPs;** **Use of bank accounts for internal transfers;** **Investing money in the purchase of property.**				
Risk description: ***It's a high risk*** ***Average probability*** ***The consequences are major***				

Conclusion – PEPs are identified as high risk, are vested with public power or dignity that provides credibility, which could lead to the concealment of suspicions. PEPs may use corporate assets, third parties, professionals, international fund transfers and international payment services to conceal the origin of criminal assets.

The risk of terrorist financing through the use of PEPs/public officials is low. This risk is also kept low by the application of know-your-customer measures by financial institutions and by supervisory controls.

Non-resident persons

In Romania, the total number of non-resident individuals is 139,502, out of which 63,591 EU citizens (other than Romanians) and 75,911 non-EU citizens.

The number of non-resident individual customers in the banks' portfolios amounts to 206,395, representing 1.05% of the total number of customers.

The number of non-resident corporate clients in banks' portfolios was 3,739, representing 0.27% of the total number of bank clients during the reference period.

Threats:

Non-resident individuals can open bank accounts or set up companies to recycle money by externalizing money using foreign transfers and/or cash withdrawals.

Vulnerabilities:

- Impediments to the identification of the beneficial owner in the case of transactions carried out through the misuse of powers of attorney granted by non-resident persons;
- The possibility to misuse an account or a company for a limited period of time followed by leaving the country, in which case tracing is difficult and involves additional costs.

Taking into account the analysis carried out for 2018 - 2020 this report has shown a low involvement of non-resident persons in money laundering offences; by adapting the banking legislation to international standards and through better enforcement of the KYC (Know Your Customer) rules, the risk of non-resident persons using the banking system for money laundering purposes has been considerably reduced.

No.	Elements	Likelihood Rating (L)	Assessment of consequences (C)	Rating of risk
	The risk of non-resident persons	**Average**	**Minor**	**Low**
Associated vulnerabilities: • impediments to the identification of the beneficial owner in the case of transactions carried out through the misuse of powers of attorney granted by non-resident persons; • the possibility of misuse of an account or company for a limited period of time, followed by leaving the country.				
Associated threat: Misuse of an account or company;				
Event description: Using a bank account for internal or external transfers; Using a company for a limited time, then closing/deactivating it				
Risk description: ***It is low risk*** ***Moderate probability*** ***Consequences are low***				

Conclusion - non-residents are at low risk, representing a low percentage of all persons convicted of money laundering. Also, this category of subjects represents a low percentage of the banks' customer portfolio, which significantly reduces the risk of using these persons for money laundering purposes. Last but not least, another mitigating factor is the additional KYC procedures applied by reporting entities to non-resident persons from high-risk countries.

With regard to the risk of terrorist financing by non-residents, we conclude that the geographical risk is low. This risk is also kept low by the application of know-your-customer rules by financial institutions and controls by supervisors.

III. ASSESSMENT OF MONEY LAUNDERING AND TERRORIST FINANCING RISKS BY ECONOMIC SECTOR

The real estate sector

Analysis of the data on money laundering convictions has indicated that one of the sectors at high risk of money laundering is the real estate sector (construction, trade of building materials, developers and estate agents).

The real estate sector is an emerging sector which has favored its use for laundering substantial amounts of money. In the period 2018-2020, 16 final sentences were handed down for money laundering offences committed through this economic sector, with a total value of €35,787,597.

The main predicate offences generating dirty money were: tax evasion; deception; embezzlement and fraud against EU financial interests.

The methods used to recycle funds in the real estate sector were internal bank transfers from resident individuals to resident legal entities followed by cash withdrawals and purchases of real estate.

In 2020, the construction industry soared significantly compared to the previous years. According to data presented by the National Institute of Statistics in 2020, the total volume of construction work increased by 16% compared to 2019 at a time when the construction industry in Europe was shrinking as a result of the COVID-19 Pandemic.

In 2020, industrial construction activity recorded the highest growth (18.5% compared to 2019) in the construction industry. The residential building construction sector also saw an increase of 17.8%, a trend also observed in previous years. Construction of bulk distribution warehouses and industrial buildings has indicated an increase of almost 11%.

In 2019, tax incentives for construction employees were introduced, with the industry showing an upward trend. The strong development of the sector recorded in 2019 was due to the substantial increase in non-residential construction of about 11%. In the year, the entire construction activity increased by 27.6%.

Real estate is a sensitive sector exposed to risks. Regulation of this sector is lax and the fact that it is an emerging sector means that there are increasing risks related to money launderers' access to the sector.

The trade in high value goods allows funds of uncertain origin to circulate rapidly in a poorly regulated market. This sector ensures anonymity of funds through the use of cash and there are no procedures to identify the beneficial owner of transactions.

USE OF ACCOUNTS HELD IN ROMANIA BY A RESIDENT LEGAL ENTITY CARRYING OUT ITS ACTIVITY IN THE REAL ESTATE SECTOR	
Description	The typology is characterized by the presence of a resident individual who receives, through personal accounts, substantial sums of money from a non-resident legal person, with the justification "invoice value". The non-resident legal person was the beneficiary of large value transfers from a resident legal person, with the justification "against consultancy contract". The resident individual transfers the amount of money received from the external party to a resident legal entity operating in the real estate market.
Profile of natural person/legal entity	The resident individual controls the non-resident legal entity and the resident legal entity has made a number of transfers to the resident individual. The resident individual provides advisory services to the non-resident legal person. After the transfer to the resident legal person, which is active in the real estate sector, the resident natural person was registered in the land register with a recently purchased high value real estate. The resident legal entity has consistently recorded losses and the consultancy contract with such a high value is not justified by the financial indicators declared by it.
Indicators (type-specific)	- The high value foreign earnings; - The purchase of a high-value asset; - External payments with the justification "consideration for consultancy contract" initiated by a company facing financial difficulties;

	- linking credits to debits on the account of a resident individual.
MECHANISM	• the use of the accounts of a resident legal person operating in the real estate market; • the use of the accounts of a non-resident legal person to conceal the illicit origin of the sums involved; • the use of the non-resident legal person's account as a transit account.
INSTRUMENT	• the use of external transfers; • the use of bank accounts;

Threats:

The real estate sector is used by organized crime groups to launder money obtained from illegal activities in Romania, especially as a result of tax evasion.

Vulnerabilities:

A specific risk in this sector is the widespread use of cash (starting with the building materials sector).

Real estate agents and developers have links with other professionals (lawyers, notaries, accountants, etc.) who pose a risk of misuse by criminals. Numerous contracts and parties are used in the real estate sector, so it is a complex activity that can facilitate the concealment of the illicit origin of money. In addition, the amounts involved are significant and allow money obtained from crime to be introduced into the legal economy.

The analysis carried out in the report revealed that there is a low level of awareness of the exposure to money laundering risk of professionals (lawyers, notaries, accountants) providing specific services in this area.

The level of awareness of money laundering or terrorist financing risks in the sector varies according to the size of the entity. Thus, small operators are not aware of their exposure to money laundering and terrorist financing risks, but large companies/those that are part of international trusts are more aware of these risks and make the necessary efforts to apply AML/CTF legislation.

The lack of coherence of the legal framework in the real estate sector is a major problem. There is a need for a coherent legal framework across the board. Given the multitude of entities operating in the sector and the multitude of activities they carry out, a specific legal framework for each of them is necessary to prevent abuse of the sector.

No.	Elements	Likelihood Rating (L)	Assessment of consequences (C)	Risk rating
	Real estate sector risk	**Average**	**Major**	**High**

Associated vulnerabilities: **Use of the underground economy;** **Use of cash;** **Poor detection of suspicious transactions (accountant, real estate agent and notary);** **Poor supervision;** **Incoherent legislation;**
Associated threat: **Tax evasion related to the real estate sector**
Event description: **Use of resident companies operating in the real estate sector;**
Investing money in cash resulting from tax evasion, especially by purchasing construction materials and paying workers in cash under collaborative contracts.
Risk description: ***It's a high risk*** ***Average probability*** ***The consequences are major***

The real estate sector is a high-risk sector due to the fact that large amounts can be transferred or invested in this sector and the level of transparency of the sector is relatively low. Also, weak legislation in the sector exposes it to a high risk of money laundering. In addition, the sector involves complex activities from the purchase of property (land), construction and sale of end products, so a wide range of service providers are used, including legal services, real estate agent services and financial services. These participants use corporate structures, often characterized by opacity.

The analysis showed that the real estate sector is not used to finance terrorism.

Agriculture

In the 2018-2020 period, the agricultural sector was identified in 11 cases in which final sentences were handed down for money laundering.

The main predicate offences were tax evasion (in 9 cases) and offences against EU financial interests (2 cases).

In these cases, the money came from frequent domestic bank transfers between resident natural persons, including persons holding local public office, and the principal method of obtaining possession of the laundered amount by the actual beneficiary was cash withdrawal.

Agriculture has been an important sector of activity in Romania's economy, but in recent years its share of GDP has declined significantly. In 2020, the agriculture sector accounted for 4% of Romania's GDP. Moreover, as revealed by an analysis carried out by the Department for Sustainable Development of Romania of the General Secretariate of the Romanian Government and published in the magazine "Economistul" (no.5(339) of May 2022), Romania is the EU Member State with the highest employment rate in agriculture, amid the paradoxical manifestation of skilled labor shortage revealed at the level of Romanian farms. According to Eurostat, in 2018, 29.4% of Romania's population worked in agriculture (while in more advanced European countries in terms of development this percentage is less than 1.5% - for example Germany).

From the point of view of the trade balance in the agricultural sector, statistical data from the NSI reveals that Romania exports raw materials and products with low added value and imports products with high added value, the trade balance thus starting to record a negative trend since 2015, one that has worsened since then. Based on this situation, one can clearly conclude that the major vulnerability of this sector is the use of cash. In rural areas, where activities in the agricultural sector predominate, the banking system is difficult to access and the banking infrastructure is poor, thus favoring the sole use of cash. The widespread use of cash in the Romanian economy is a major risk highlighted in the literature[8]. Therefore, the use of cash can create the possibility of money laundering, while preserving anonymity and making it impossible to trace funds.

The use of cash in agriculture is facilitated by:

- the use of poorly educated labor force whose payment is made exclusively through the use of cash;
- the seasonal nature of the work carried out in the agricultural sector, favoring informal work without an employment agreement and paid in cash;
- carrying out the activity in this sector in rural areas where cash is mainly used.

Threats:

The agricultural sector is easy to access by anyone involved in money laundering because of the intensive use of cash, and banking operations are rarely used, especially in cases involving large companies or purchases of agricultural machinery/land for which cash limits are imposed by law. In this context, it is easy to get money into the system without controlling its origin. These financial transactions take place outside the banking system and can no longer be verified by compliance officers or subject to know-your-customer measures applied by financial institutions.

Vulnerabilities:

Activity in this sector involves the use of cash labor and even raw materials that are paid for in cash.

Awareness of the risk of money laundering or terrorist financing in this sector is almost non-existent, with the majority of participants in agricultural activity having a low level of education.

There are many farms in Romania, but most of them are subsistence farms. However, large farms do involve large sums of money for the purchase of land or equipment, which could facilitate the use of money obtained from illegal activities. It is also well known that in agriculture, large farms (a small percentage of farms) are owned by foreign nationals or foreign legal entities operating in the sector, which could facilitate the use of foreign funds without the possibility of obtaining information on the origin of the money or identifying the real beneficiary.

In this area, there are many grants that could be misused by the beneficiary in the absence of adequate supervision and controls by the authorities.

8 https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/963637/Final%20%20%20%20%20din%20Revizuit%20mL%20TF%20Risk%20Factors.pdf

The underdeveloped banking network in rural areas is a determining factor in the widespread use of cash in this area.

Accounting in this sector allows for the use of cash, and these transactions are based on legal documents completed by individuals and are bank supporting documents.

No.	Elements	Likelihood Rating (L)	Assessment of consequences (C)	Risk rating
	Risk in the agricultural sector	**High**	**Moderate**	**Average**
Associated vulnerabilities: **Use of cash;** **Lack of detection of suspicious (accounting) transactions;** **Poor supervision in terms of accessing funds from the European budget or the national budget;**				
Associated threat: **Tax evasion related to agriculture**				
Event description: **The use of enterprises operating in the agricultural sector;** **Use of foreign capital;** **The investment of cash was the result of tax evasion, especially through the purchase of materials and payment of workers.**				
Risk description: ***It is a medium risk*** ***High probability*** ***The consequences are moderate***				

The agricultural sector presents a medium risk, mainly due to the use of cash and the possibility of accessing subsidies from the EU or the national budget that are used for purposes other than those for which they were granted. In addition, awareness of the risk of money laundering through the sector is limited.

The rural population is the main participant in the activities of the agricultural sector and the structure of rural society in Romania is not suitable for financing terrorist acts.

The analysis showed that the agricultural sector is not used for terrorist financing.

Oil and natural gas trading sector

In the period 2018-2020, 7 final convictions for money laundering were handed down in the oil and gas sector.

In the cases mentioned above, the main crime that generated the money laundered was tax evasion.

The recycling methods used were internal and external bank transfers, followed by cash withdrawals.

Historically, the oil and gas sector in Romania has made a substantial contribution to gross domestic product (GDP), but in the current period this contribution has started to decrease due to several factors (e.g. declining reserve replacement rates). Following the trend to

replace fossil fuels with alternative fuels (renewable energy), the role of this industry is continuously decreasing.

Between 2007 and 2019, the total impact of oil and gas companies operating in the economy was around 5.9% of GDP.

Even in this context, the fuel trade is extremely attractive to money launderers due to the fact that these products are subject to excise duty and taxes, which allows them to obtain a substatement of the sale of products without paying these taxes and duties and to reinvest the profits obtained illicitly in this sector as well.

The sale of petroleum products involves the collection of additional taxes and other excise duties, which makes it easier for traders to engage in tax evasion, a trend also identified at EU level.

USE OF ACCOUNTS HELD IN ROMANIA BY LEGAL ENTITIES RESIDENCES FOR THE RECYCLING OF MONEY OBTAINED FROM CRIMES IN THE MARKETING OF PETROLEUM PRODUCTS	
Description	The typology is characterized by the presence of a group of resident legal entities which have received amounts in the order of tens of millions of EUR from non-resident legal entities with the justification "Invoice countervalue for petroleum products". The resident legal persons were coordinated by non-resident individuals from the same jurisdiction as the non-resident legal persons. Once the money was received, it was immediately transferred to the Asian jurisdictions.
Profile of natural person/legal entity	Non-resident legal persons have been involved in tax evasion involving petroleum products in the jurisdiction in which they are registered. The resident legal persons did not carry out a real economic activity and the object of their activity was the marketing of petroleum products. The accounts of the resident legal persons were used for the transit of the illegally obtained sums. Resident legal persons also failed to submit the tax declarations required by the legislation in force.
Indicators (type-specific)	- high-value foreign receipts and payments made repeatedly; - correlation of the credit with the debit of the accounts of resident companies; - information regarding the involvement of non-resident legal entities in the crime of tax evasion in the sale of petroleum products;
MECHANISM	• using the accounts of resident legal entities to carry out operations involving amounts from untaxed commercial activities; • using accounts belonging to legal entities to transfer money to jurisdictions in the Asian area;

	• the use of company accounts as transit accounts
INSTRUMENT	• the use of external transfers; • use of bank accounts;

Threats:

Organized crime groups could use the sector to hide the illicit origin of money, as the commercial operations carried out in this sector involve large sums of money. Also, the contracts used in this economic sector are complex contracts which most of the time have an extraneous component, making it difficult to trace the money.

Vulnerabilities:

- the involvement of large sums of money;
- the possibility of avoiding payments to the state budget involving substantial amounts;
- the awareness in this sector is almost absent,
- the involvement of an element of foreignness. In most cases "off-shore jurisdictions" are involved;
- the poor quality or lack of controls by state authorities regarding tax and money laundering regulations.
- there are many cases of smuggling in this sector.

No.	Elements	Probability assessment (IT)	Assessment of consequences (C)	Risk rating
	The risk in the oil products and natural gas marketing sector	**Average**	**Moderate**	**Average**
Associated vulnerabilities: **Use of electronic transfers;** **Use of Internet banking services;** **Deficient/gap checks performed by the tax authorities.**				
Associated threat: **Fiscal evasion in the sector of the marketing of petroleum products, oil and natural gas;** **Smuggling**				
Event description:				

Use of resident companies in the oil and natural gas trading sector. **Money collected from abroad through external transfers;** **Use of ghost companies.**
Risk description: ***It is a medium risk*** ***Average probability*** ***The consequences are moderate.***

The oil and gas trading sector has a medium risk and the most common predicate offence was tax evasion. Sometimes this sector is linked to smuggling of goods and the amounts involved are substantial.

The oil and gas trading sector is not attractive for terrorist financing, due to the fact that all transactions are carried out through the banking system, which is well aware of the risk involved in high-risk jurisdictions and which has implemented adequate KYC measures. In conclusion, the risk of terrorist financing is classified as low.

Commercial activities

In the trade sector, 17 cases of money laundering offences were identified and the predicate offences identified in the above cases were tax evasion, fraud and embezzlement.

Tax evasion is the main predicate offence in the trade sector.

The trade sector in Romania accounts for 18% of the Gross Domestic Product (GDP), worth RON 189,200 million, which shows that it is an important economic sector offering the possibility to recycle substantial amounts of money.

E-commerce experienced significant growth during the COVID-19 pandemic. In 2020, this sector has seen the highest growth, with Romania ranking first among the countries of South-East Europe, which has led to the use of this sector by money launderers.

According to a study published by the renowned e-commerce platform Ecommerce Germany News[9], 15 million consumers in Romania shop online. They surf the Internet for about 7 hours and 21 minutes on average per day. Of the 15 million people, 11 million are active users on social media platforms, 98% of whom access these platforms from their mobile phones. The European E-Commerce Report 2022 (prepared by the Centre for Market Insight of the University of Applied Sciences in Amsterdam at the request of Ecommerce Europe and EuroCommerce)[10] reveals that in Romania, e-commerce turnover is estimated at €6.2 billion in 2021, up 11% compared to 2020, and the sector is expected to grow by 13% to €7 billion in 2022.

In practice, e-commerce-specific transactions in Romania accounted for almost half of the Eastern European total in 2021, estimated at €14 billion.

E-commerce accelerates high value transfers due to the predominant use of Internet banking and online card payments. At the same time, these payment instruments offer the advantage of anonymity in terms of the beneficial owner of the funds transferred and anonymity of the source of funds.

[9] https://ecommercegermany.com/blog/european-ecommerce-overview-Romania

[10] https://ecommerce-europe.eu/wp-content/uploads/2022/06/CMI2022_FullVersion_LIGHT_v2.pdf

Threats:
Money launderers could use this sector to hide the illicit origin of money, taking advantage of the anonymity and speed of transactions in this sector.

Vulnerabilities:

- The use of complex structures, including shell companies, to develop business activities;
- The use of accounts/companies established in high-risk jurisdictions in commercial activities;
- The use of inactive companies;
- The use of newly established or recently reactivated companies used in commercial activities with a high volume and significant values;
- The use of INTERNET banking payments in e-commerce to avoid interaction with bank officials and to avoid the use of supporting documents.

No.	Elements	Probability assessment (IT)	Assessment of consequences (C)	Risk rating
	The risk in the trade sector	**Average**	**Moderate**	**Average**
Associated vulnerabilities: **Use of external transfers;** **Use of Internet banking services;** **Use of a newly established or recently revived company engaged in high-volume, high-value commercial activities;** **Use of "ghost" companies.**				
Associated threat: **Tax evasion, fraud and misappropriation of funds;**				
Event description: **Using resident companies for fraudulent money transfer;** **Cash withdrawal of fraudulently obtained money.**				
Risk description: ***It is a medium risk*** ***Average probability*** ***The consequences are moderate.***				

The trade sector presents a medium risk due to the fact that most companies or authorized individuals are registered in the national trade register and hold bank accounts, in both cases the business entities are under the supervision of the competent authorities. Moreover, the vast majority of commercial operations intersect at some point with the banking system, and are supported by the performance of financial-banking operations, which leads us to the application of know-your-customer rules within financial institutions, these operations falling under the scope of oversight by financial institutions.

The trade sector is classified as low risk from the point of view of terrorist financing for the reasons mentioned above.

IV. ASSESSMENT OF MONEY LAUNDERING AND TERRORIST FINANCING RISKS BY FINANCIAL SECTOR/PRODUCT

4.1. General conclusions of the sectoral assessment

The banking sector presents an average residual risk, mainly due to the most complex and mature control environment compared to the rest of the obliged entities.

The overall risk of the non-bank financial institutions (leasing/lending) sub-sector is low due to the limited nature of the products, the low geographical coverage and the fact that most entities have resident clients in their portfolio and offer low value leases and loans.

The sub-sector of institutions issuing electronic money presents an average-high risk. The classification in this level of risk was due to the identified deficiencies.

The payment institutions sub-sector was assessed as medium-high risk, mainly due to the identified weaknesses.

The e-money distributors/paying agent sub-sector is considered medium-high risk due to the lack of oversight tools, the number of agents and the lack of a culture of compliance.

With regard to financial instrument intermediaries, investment agents/delegates, investment fund management companies, as well as financial instrument depositories, it was found that these entities present an average residual risk of being used for the purpose of money laundering. At the same time. It appears that financial insurance institutions present an average risk of being used for money laundering purposes (for life insurance and unit link/annuities).

The sector of pawnbrokers (non-bank financial institutions registered in the National Bank of Romania's register) and non-bank financial institutions (registered exclusively in the National Bank of Romania's general register and not having the status of payment institution or electronic money institution) present a medium risk of being used for money laundering purposes, as does the foreign exchange sector. At the same time, the mutual aid houses sector (non-bank financial institutions registered in the National Bank of Romania's register) presents a low risk in terms of money laundering threat.

The gambling services provider sector presents a high risk of being used for money laundering purposes, both in terms of casinos (land-based or online) and online gambling. For gambling service providers (land-based) and slot machines (land-based), the risk level is medium.

Professionals such as lawyers, notaries, chartered accountants and accounting experts as well as tax consultants are exposed to a medium risk of being used for money laundering, whereas other professionals such as auditors and appraisers are at low risk.

The level of money laundering threat related to legal professionals is also considered to be medium for insolvency practitioners and low for bailiffs.

The level of money laundering threat related to the services provided by management and business advisory professionals is considered high.

Providers of services to companies or trusts, other than those referred to in points (e) and (f) of Law 129/2019, present a high risk of being used for money laundering purposes.

The level of money laundering threat related to real estate agents and developers is considered high and persons trading art present a medium risk.

Providers of virtual currency and fiat currency exchange services and providers of digital wallets present a high risk of being used for money laundering purposes.

Sector of financial entities supervised by the National Bank of Romania

4.2.1. Overview of the sector

Entity Categories

The National Bank of Romania (NBR) has exclusive responsibility for risk-based supervision and control of compliance with the legal framework on preventing and combating money laundering and terrorist financing by the following categories of financial institutions[11] that carry out their activity and have a physical presence on the territory of Romania:

a. credit institutions: Romanian legal entities and branches of credit institutions of foreign legal entities (35 entities: 23 banks, 2 housing savings and lending banks, a credit cooperative organization and 9 branches of credit institutions from other states limbs);
b. payment institutions: (9) Romanian legal entities and (2) branches of payment institutions from other member states (11 payment institutions in total);
c. electronic money issuing institutions: (2) Romanian legal entities and (3) branches of electronic money issuing institutions from other member states (a total of 5 electronic money issuing institutions);
d. non-bank lending/leasing financial institutions (NBFI) registered in the Special Register: (74 entities – of these, 4 institutions are also authorized as payment institutions, and one is also authorized as an electronic money issuing institution).

In the case of the institutions referred to in points (a) to (c) Romanian legal persons, the NBR shall also have the power to supervise and control the activities carried out by them directly in the territory of another Member State.

In addition to this full supervisory competence, the NBR supervises, as host supervisor, on a risk basis, whether the activities carried out through agents and distributors in Romania of electronic money issuing institutions and payment institutions from other Member States comply with the legal requirements on the prevention and combating of money laundering and terrorist financing.

The banking system is the main player in the financial system with the largest market share and also offers a much wider range of financial products and services with the best international interconnectivity.

[11]Registered at the end of 2020;

Supervisory skills and tools

It is important to underline, in order to understand the approaches and tools used by the Central Bank in its capacity as a supervisory authority in the field of preventing and combating money laundering and terrorist financing, that the NBR is empowered by law only to verify compliance of the supervised entities with the provisions of the legal framework on the prevention and control of money laundering/terrorist financing, without actually having any tasks related to the analysis/investigation of money laundering/terrorist financing cases/transactions. In these circumstances, the NBR is not legally empowered to receive Suspicious Transaction Reports (STRs) from supervised entities, as these tasks are related to the NOPCML. Consequently, the guidance on the ML/TF typologies that may be developed internally by the NBR is largely based on information received from other authorities receiving, analyzing or investigating such information/cases and/or from external public sources.

The main supervisory actions carried out by the NBR on supervised institutions aim to determine whether:

(a) the risk assessment methodology and its implementation adequately cover all categories of customers, products and services, distribution channels, geographical areas, as well as the overall activity of the supervised institution and that they are sufficiently documented and updated, whenever necessary;
(b) specific control systems and procedures are in place to verify that its own risk assessments are relevant and comprehensive/appropriate and that the results of related audits are communicated to management and followed up with appropriate corrective actions;
(c) its own risk management policies and procedures are appropriately linked to the determination of the set of customer due diligence (CDD) measures applicable to each client;
(d) the rules are applied effectively and the way they are applied is not formal in the sense that they are not only aimed at avoiding legal risk by ticking certain requirements, but fulfil the purpose of the field of preventing and combating money laundering and terrorist financing to ensure appropriate preventive measures;
(e) the identification of customers/actual beneficiaries is carried out in accordance with the requirements of the regulatory framework;
(f) financial institutions do not initiate a transaction when they have not been able to apply all know-your-customer measures/establish the legitimacy of the purpose and nature of the business relationship/manage the risks;
(g) financial institutions shall have arrangements in place for regular verification of both the veracity and adequacy of information held on customers, including the beneficial owner, commensurate with the level of risk associated;
(h) financial institutions apply, in addition to standard know-your-customer measures, additional know-your-customer measures in all situations which, by their nature, may present an increased risk of money laundering or terrorist financing;
(i) financial institutions conduct adequate, documented and formalized monitoring of transactions and business relationships to detect unusual or suspicious transactions;
(j) financial institutions submit a suspicious transaction report to the NOPCML whenever there are grounds for suspicion (based on analysis of samples and red flagged transactions);
(k) financial institutions implement effective and appropriate IT systems covering all financial activities, the entire customer portfolio and all transactions that pose associated money laundering or terrorist financing risks and monitor, collect and

analyze data on money laundering and terrorist financing risk to facilitate appropriate internal and external reporting;

(l) financial institutions shall designate persons with responsibilities for the implementation of anti-money laundering and combating terrorist financing and money laundering requirements and the nature and limits of the responsibilities assigned;

(m) financial institutions shall ensure regular training/verification of employees accordingly, establish and document appropriate standards in the recruitment process;

(n) the requirements of Regulation (EU) No 847/2015 on transfers of funds are properly implemented.

In this context, information collected by the NBR in relation to suspicious activity/transactions may only arise if something is detected in the analysis of the sample of transactions/customers used for the compliance check. It is important to emphasize that such a detection may be a potential outcome of the verification, but not an aim, given the role of the supervisor as defined by law and the tiny percentage of transactions that can be reviewed by the supervisor compared to the total volume of transactions conducted by a bank/institution. However, if the NBR, in the exercise of its specific duties, discovers facts that could be related to money laundering or terrorist financing, it immediately informs the NOPCML, but without being involved in further analysis or knowing whether suspicions have been confirmed, also taking into account the time horizon required to go from suspicion to a final conviction, the evidence that could/could not be obtained, etc.).

The NBR, as Romania's central bank, is both the supervisory authority in the field of preventing and combating money laundering and terrorist financing and the prudential supervisory authority for the categories of financial institutions listed above (with the exception of the prudential supervision of branches of institutions in other Member States). Complementary to its supervisory activity, the NBR, as licensing and prudential supervisor (in cooperation with the Money Laundering and Terrorist Financing Prevention and International Sanctions Supervision Service), verifies the fulfilment of fit and proper criteria for shareholders, beneficial owners and members of governing bodies, including compliance officers.[12.] The supervised entity/acquirer must provide the NBR, in a timely and accurate manner, with all information necessary for the assessment of fit and proper in all cases (new appointments, changes in circumstances, changes in role, etc.). The supervision of fit and proper criteria must prevent persons who would pose a risk to the proper functioning of the governing body from entering or continuing their role in the first place when a fit and proper issue has arisen. In order to grant authorization to a Romanian legal person credit institution, the NBR must be informed of the identity of the shareholders or associates - natural or legal persons - who will hold, directly or indirectly, qualifying holdings in the credit institution concerned, and of the value of these holdings. The NBR shall grant authorization only if, having regard to the need to ensure the sound and prudent management of the credit institution, it is satisfied as to the suitability of such persons. Any potential acquirer shall give prior written notice to the NBR of any proposed acquisition, indicating the target threshold for capital ownership and providing all relevant information required by law. In order to assess the quality of the persons and entities involved in or related to the submitted

[12]Government Emergency Ordinance No 99/2006 on credit institutions and capital adequacy, approved with amendments and additions by Law No 227/2007, with subsequent amendments and additions; NBR Regulation No 5/2013 on prudential requirements for credit institutions, as amended and supplemented, which includes the provisions of the Guideline on the assessment of the suitability of members of the management structure and key persons (EBA/GL/2017/12);
NBR Regulation No 12/2020 on the authorisation of credit institutions and amendment of their statutes.

authorization project, upon request of the NBR, the NOPCML shall provide information on the risk of money laundering or terrorist financing in relation to the persons or entities concerned. Other authorities are also consulted and information is obtained from public institutions in Romania and from other national and international supervisory authorities.

The NBR rejects an application for authorization if it is not satisfied as to the suitability of the shareholders, the beneficial owners, the directors and/or managers of the credit institution because the reputation, honesty and integrity of the person or their professional expertise are not appropriate to the nature, scale and complexity of the credit institution's business or are not consistent with the need to ensure prudent and sound management.

The NBR assesses the suitability of the potential acquirer against a number of criteria, including its reputation, i.e. its integrity, reputation, professional competence and experience of any person discharging managerial and/or administrative responsibilities within the credit institution as a result of the proposed acquisition and whether there are reasonable grounds to suspect that a criminal offence or attempted criminal offence of money laundering or terrorist financing has been committed in connection with the proposed acquisition. In this respect, the NBR applies the Joint Guideline[13] on the prudential assessment of acquisitions and increase of qualifying holdings in the financial sector JC/GL/2016/01, which harmonizes the conditions in the EU under which the potential acquirer of a holding in a financial institution is obliged to notify its decision to the competent authority responsible for prudential supervision. The assessment is carried out in accordance with the relevant provisions of the sectoral directives and regulations which require as a condition for the granting of authorization that the persons who will run the institution are "fit and proper" on the basis of the documents provided, information requested from the NOPCML, other supervisory authorities, previous employers, etc.

The assessment of the suitability of these persons shall be carried out in accordance with the EBA Guidelines on the assessment of suitability of members of the management structure and key persons.

The same approach, based on specific legislation, applies to all other categories of financial institutions supervised by the NBR.

The supervisory model in the area of prevention of money laundering and terrorist financing used by the NBR for entities supervised for prudential purposes is characterized by the so-called external model, as classified in the material entitled "The Economic and Legal Effectiveness of Anti Money Laundering and Combating Terrorist Financing Policy Final Report"[14] carried out under a project funded by the European Commission. The main advantage of this model is the existence of sound sectoral knowledge. Thus, within the NBR, since 2009, in order to improve the specialization and targeting of inspections, a specialized structure has been created within the Supervision Directorate, now called the Service for the Supervision of the Prevention of Money Laundering and Terrorist Financing and the Application of International Sanctions.

[13]The common guide of the European Supervisory Authorities (European Banking Authority, European Authority for occupational insurance and pensions and the European Securities and Markets Authority);

[14] http://www2.econ.uu.nl/users/unger/ecolef_files/Final%20ECOLEF%20report%20(digital%20version).pdf – "The final report on the economic and legal effectiveness of the policy to combat money laundering and financing *terrorism*"

The structure of the National Bank of Romania specialized in the field of prevention of money laundering and terrorist financing cooperates internally and benefits from technical assistance, as appropriate, from other relevant departments, such as the Legal Directorate, the Regulatory and Authorization Directorate, the IT Services Directorate, etc.

Continuous assessment of ML/TF risks

Since 2017, the NBR has initiated a risk assessment process to estimate the risk of supervised entities. Each institution is assessed on the basis of a process that involved analyzing the information received through the questionnaire sent to supervised entities for this purpose, correlated with the findings of inspections and off-site monitoring activities. These ratings are used for the annual planning of on-site supervision in the area of prevention and combating money laundering and terrorist financing.

Both exogenous risk factors for the sector and endogenous risk factors intrinsic to the sector under review are taken into account. Various questionnaires, sent out each year to address new issues, have provided an opportunity to update the view of the sector and cross-check the information provided. The overall picture is adjusted on the basis of the exchange of relevant information (a continuous cooperation with the prudential supervision services as they are part of the same directorate), with particular emphasis on operational risk and internal control weaknesses. In fact, in recent years there have been cases where the supervisory and evaluation process - the assessment of SREP by prudential supervisors[15] have been influenced by the risk of money laundering and terrorist financing, an issue that has just started to be formalized at EU level. In addition, there are exchanges of information with NAFA and NOPCML. In accordance with the provisions of the legal framework in force, the NBR cooperates with all competent national authorities.

Annually, based on the results of the risk assessment at the sector/sub-sector/entity level covered by supervision, the NBR reviews and, where appropriate, revises the objectives of the supervisory actions so that they are appropriately calibrated.

From 2020 onwards, the questionnaires used have been designed separately for each sub-sector, distinguishing between different types of financial institutions.

These questionnaires, in addition to providing the NBR's supervision with a picture of the system itself, provide cross-checking information to identify how supervised entities manage perceived risk and the level of effective understanding of the requirements, not only to assess compliance, but also the quality of entities' anti-money laundering and anti-terrorist financing policies and procedures, as well as risk appetite. Supervisory staff come from different areas such as prudential supervision, compliance or other departments specializing in different internal control functions within commercial banks, the NCBPBS, the specialized police unit on economic crime investigation, etc.

According to the latest version of the supervisory procedure[16] in the area of prevention of money laundering and terrorist financing (November 2021), the strategy has been improved to increase the efficiency of the use of resources. The off-site component of the NBR's AML/CTF Service is mainly responsible for the elements taken into account in the risk

[15] SREP - Supervisory Review and Assessment Process

[16] on the supervisory review and risk-based assessment of credit institutions, non-bank financial institutions, payment institutions and electronic money institutions in relation to their exposure to money laundering, terrorist financing and international sanctions risk

profile, such as the business model or the analyses of banks' internal procedures, while the on-site structure carries out the checks to be performed on-site.

Off-site assessments are not limited to the monitoring of key risk indicators, sources taken into account when updating the risk profile of financial institutions include negative media reports, complaints, referrals, new products or new alternative channels launched by supervised institutions, changes in their business strategy, information from internal or external audits of supervised entities, information from NOPCML/other authorities. Based on this data, internal assessments are issued with proposals for further action (e.g. drafting a supervisory report, requesting additional information and documents from the bank or other institutions (if the information reveals risk factors related to other institutions, setting up meetings with key staff, taking the findings into account when updating the individual risk profile and so on).
Three strategic priorities have been defined for 2021, the first two of which are included in the objectives of each planned supervisory action for 2021:

1. Implementation of the current AML/CTF regulatory framework/international sanctions enforcement by supervised institutions and recommendations transmitted to the system during 2020, including from the perspective of ML/TF/international sanctions evasion risks generated by the COVID pandemic,- with 3 components:
    - The Assessment of the methodology for conducting and updating the risk assessment implemented by the supervised institutions, how it is implemented, and the policies developed to manage and mitigate the risk of money laundering and terrorist financing and circumvention of international sanctions to which the institution is or could be exposed, respectively;
    - The assessment of how the recommendations submitted to the system were implemented in 2020;

2. Verification of the implementation of the provisions of Regulation (EU) 2015/847 of the European Parliament and of the Council of May 20th, 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006, management of the ML/TF risks associated with increasing digitization, adoption of FinTech/new technology solutions, increasing cybercrime during the pandemic and weaknesses in the IT systems used in the Know Your Customer business, prevention of money laundering - with 3 components:
    - The assessment and implementation of the digitization strategies and their impact on business models and implications on internal governance and internal control system (establish a sound and effective governance culture of ML/TF risks associated with implementation of digitization strategies, adoption of FinTech/new technology solutions, the rise of cybercrime during the pandemic and the weaknesses of IT systems used in the KYC, ML prevention and counter-terrorism financing business and a robust internal control system, in particular in terms of risk assessment, accurate customer identification and quality of data collected at the time of business relationship initiation, established KYC measures and transaction monitoring).
    - The assessment of the ML/TF risks associated with digitization projects to enable remote access for both individual and corporate customers and to provide digital services and solutions;
    - The ML/TF risks arising from reliance on digital and remote solutions to conduct day-to-day operations and provide services to customers.

3. Raise awareness of emerging risks, i.e. new ML/TF/bypassing international sanctions typologies, in the context of a potential new economic crisis and with a view to updating risk assessments accordingly.
    - Work with supervised institutions, NOPCML and judicial bodies to identify and raise awareness of emerging risks, i.e. new ML/TF/bypassing international sanctions typologies, in the context of a potential new economic crisis and to update risk assessments accordingly.

These actions aim to identify the most important sources, causes, risks and interdependencies between them in order to provide a thorough understanding of the sector, sub-sector and financial entity being supervised, to adjust the strategy, not only in terms of supervisory actions, but also to make proposals for changes to the regulatory framework, procedures and regulatory tools.

Inherent money laundering/terrorist financing risk factors

The risk assessment in this regard is consistent with the requirements of the risk-based approach in line with GAFI (FATF) Recommendation 1.

With regard to inherent risk factors, a distinction is made between exogenous and endogenous risks/vulnerabilities, with NBR supervision being able to influence only the second category in order to increase the resilience of financial institutions. Resilience/risk mitigation measures relate to the effectiveness of available policy instruments to prevent money laundering and terrorist financing. This refers both to the content/scope of policy instruments and the implementation of these instruments (existence of policies, controls and procedures in place to adequately manage identified money laundering and terrorist financing risks commensurate with the nature and size of the reporting entities concerned). Resilience can determine the likelihood of occurrence of threats and the extent of their potential impact. The principle is - the greater the resilience/risk mitigation measures, the better the threats will be addressed. While inherent risk factors and sometimes vulnerabilities consist of factors that are relatively insensitive to policy changes, the resilience element comprises factors that can be influenced. In fact, the purpose of risk assessment is to support specific policy decisions and the implementation of those decisions that can help prevent the occurrence of money laundering and/or terrorist financing.

The approach combines qualitative and quantitative information and professional expertise. Data was collected from a variety of international and national sources (public and private), including international studies and reports, statistics and data not publicly available from surveillance work. This was complemented by expert advice through regular high-level interactions with the authorities concerned and the private sector to enrich the findings. In line with a conservative approach, risk assessment was considered better where statistics or detailed knowledge were lacking. Where appropriate, a lower level of granularity is applied for a sub-sector level assessment.

Regarding the presence of illicit funds in the financial landscape in Romania, based on the responses received from the inspectors general of the NBR's Money Laundering and Terrorist Financing Prevention and International Sanctions Enforcement Service, who, using their professional assessment and opinion, expressed their views to estimate the threats and vulnerabilities related to the supervised sector and based on the responses to questionnaires received from the supervised entities, the following conclusion can be drawn:

In addition to the threats and vulnerabilities already outlined in the NRA, the sector supervised by the NBR is exposed to money laundering and/or terrorist financing risks arising from the following inherent factors:

- the nature of products offered to customers; (banks and payment institutions)
- the geographical area covered; (banks and payment institutions)
- the variety of products offered to customers (banks);
- the heterogeneity of the customer portfolio;
- the increasing speed of access to services (banks, PIs, EMIIs);
- the rapid development of new products and distribution channels, under pressure from FinTech;
- the ongoing changes in ML/TF trends and typologies (banks, PIs, EMIIs); and
- the difficulties generated, in some cases, by GDPR, in relation to certain customers in terms of updating KYC information;

The threats of money laundering and terrorist financing are different in nature and this is taken into account, so the NBR has taken steps to continuously improve awareness of all legal obligations related to this risk. It should be noted that both the findings of the supervisory activities and the information received from other authorities and available intelligence did not indicate a major threat to the financial sector supervised by the NBR.

In order to identify terrorist financing risks/related vulnerabilities in NBR inspections, data are requested on cross-border transactions, occasional transactions (remittances) and sample checks are carried out on transfers to and from high-risk jurisdictions, online transactions from PIs located in high-risk countries, customers who repeatedly transfer or cash small amounts of money to/from different persons associated with high-risk countries, NGOs, etc.

Surveillance activities assess the scenarios implemented for monitoring transactions, how parameters are set in the screening application and perform effective detection tests to ensure that the scenarios are tailored to the customer portfolio and type of financial institution assessed. Also, as part of this activity, both the internal control systems related to the management/filtering of suspicious transaction alerts as well as the analysis performed by compliance staff for closed alerts (without STRs) to identify potential instances of non-compliance are subject to review. These checks under the NBR's legal powers were more focused on assessing the functioning, efficiency and coverage of the systems in general, and not on specific transactions, as the central bank does not play an active role in any investigation.

In conjunction with the supervision and monitoring activities, in order to support reporting entities in fulfilling their legal obligations, the NBR regularly sends risk awareness letters to the system related to red flags/indicators such as the use of terms in transaction details, identification of beneficial owners, derisking, risks posed by straw men used in company formation, opening of bank accounts and processing of transactions, as well as on risks related to offshore companies.

Subsequently, during inspections, the measures implemented as a result of these disclosures are checked. Targeted financial sanctions (TFS), the listing of organizations and individuals under an international counter-terrorism sanctions regime, is one of the preventive measures against terrorist activities (and also those related to the financing of nuclear proliferation).

In addition to the prevention of terrorist financing through the use of the international sanctions list, another means / component is the implementation of the requirement set out in the NBR Regulation No. 2/2019 on preventing and combating money laundering and terrorist financing to establish, for all customers and for all transactions, regardless of their risk categories, systems to detect complex and/or unusual/suspicious transactions, including from the perspective of how transactions are carried out in relation to the customer risk profile determined by the institution, using metrics and models, aimed at detecting any circumstances/elements that may raise questions about the nature, purpose or motivation of the transaction, such as the existence of certain anomalies compared to the customer profile (the analysis of the CTF domain from the perspective of the sector supervised by the NBR is also presented in the final part of this document).

Overview of ML/TF threats

The matrix used for the sectoral assessment:

Threat factors	**Low threat**	**Medium threat**	**High threat**
ACCESSIBILITY e.g., accessibility and relative cost	**Difficult -** it is difficult to access and/or it may cost more than other options.	**Moderate Reasonably accessible** and/or a viable option from the financial point of view	**Easy Widely accessible** and available through a lmodest means and/or at relatively low cost
EASE OF USE *e.g,* technical knowledge and/or expertise and necessary support	**Difficult** It requires more planning, knowledge and/or technical expertise than other options.	**Moderate** Requires moderate planning; technical knowledge and/or expertise.	**Easy** Relatively easy to use; little planning, little knowledge and/or technical expertise required compared to other options.
THE DISSUASIVE EFFECT *e.g,* existence of AML and/or other barriers in the way abuse	**Significant** Discouragement measures and controls exist and are reasonably effective to discourage ML/TF.	**Limited** measures of discouragement and controls have a certain effect deterring the criminal use of the service.	**Reduced (weaker)** Limited or it does not work as intended.
DETECTION *e.g.,* capacity of to identify and report to the authorities ML/TF transactions/activities	**Likely** A range of money laundering methods is visible and detectable.	**Limited** A number of money laundering methods can be identified, but the reporting is limited and large volumes of fund flows limiting detection.	**Difficult** Detection is difficult and there are few financial or other indicators of suspicious activity.

INTENT *e.g ,* attractiveness perceived for money laundering through this system	**Low** perceived as relatively unattractive and/or unsafe.	**Moderate** Perceived as being of moderate attractiveness and/or quite safe.	**High** Perceived as attractive and/or safe.

This matrix is useful for assessing and differentiating sectors and different products/services which, due to their characteristics, present a higher risk/opportunity for certain criminal activities. However, the results are presented in a broader picture, including information from surveillance actions, typologies, etc.

According to the classification in the matrix above, the overall picture of the financial sector supervised by the NBR shows that it offers accessibility at a reasonable cost, which increases risk. However, the size of the system and financial flows is quite small at EU level, so large amounts are easy to detect. Also, the accessibility in terms of the international network and complex products cannot be compared to that offered by international financial centers.

From this point of view, the banking system is reasonably accessible and a financially viable option, which is a medium threat. In terms of ease of use, it requires moderate levels of planning, knowledge and/or technical expertise, so is also considered a medium threat. Suspicious transactions illustrate that the average criminals do not use the banking system for laundering or transferring, as such transactions are usually the result of the actions of international networks specialising in internet fraud, etc. Deterrent measures and controls are in place and reasonably effective and significantly discourage money laundering, which is a factor that reduces the overall risk. High level of know-your-customer requirements, documentation and formalities, continuous updates and monitoring, combined with a predominantly domestic customer base, reduce the possibility of abuse.

The high share of STRs from the financial sector supervised by the NBR (predominant in the total number of STRs) illustrates a good capacity to identify and report money laundering to the authorities, so that detection has a low threat impact. As a result of the NBR's focus on verifying transactions that have been flagged by IT systems or that have posed a high risk on customer samples, on scenarios for detecting suspicious activity, on the quality of suspicious transaction analysis, on the adequacy of training received by employees of regulated entities under NBR supervision, etc., the number of STRs reported by the sector has increased in recent years, as has the number of ex-ante STRs (submitted prior to the transaction taking place). According to the NOPCML report for 2020 (http://www.onpcsb.ro/pdf/rapact2020.pdf), 2020 also saw an 81.63% increase in the number of cases that had transactions suspended (compared to 2019), due to an increase in the number and quality of ex-ante STRs.

Thus, there is an intention to use financial services. However, due to the factors explained above, it is perceived as moderately attractive and/or quite safe. Among the sub-sectors supervised by the NBR, it can be observed that the sub-sector of non-bank lending/leasing financial institutions presents the lowest risk of money laundering/terrorist financing. This is due to the fact that the customer portfolio is almost entirely made up of residents and the amounts processed through these financial institutions are quite small, and due to the nature of the products offered (loans, leasing). Although in other countries loans have been used for

terrorist financing activities, there are no indications that such cases have been recorded in Romania.

The payment institutions authorized by the NBR operate mainly in Romania, with no branches or subsidiaries abroad, and only 2 entities have transferred their activities to other Member States (one EMII and one PI, both Romanian legal entities), but at the end of 2020 none of them was actively providing services in other Member States. This, together with the limits of transfers, clearly reduces accessibility and intent on this level. The 2 main remittance players with a global reach, as indicated by transaction flows, are very active, especially in jurisdictions with large Romanian migrant communities. The risk should not be underestimated; vulnerabilities are related to the fact that a business relationship is not formed with clients and that information on the client's source of funds is limited. In addition, in the case of non-resident clients, there are increased difficulties in verifying the data provided by clients - e.g. address, as this is not available on passports, and an increasing number of countries also exclude this information from national identity documents. However, these factors are similar for most jurisdictions.

Vulnerabilities in the sector supervised by the NBR

Endogenous risks are vulnerabilities related to the supervised institution, its policies, procedures and prevention systems, which may increase the risk of misuse for money laundering and terrorist financing purposes.

Deficiencies consist of ineffective enforcement (an application of a AML/CTF requirement or policy in a manner that is considered ineffective or inappropriate and which by its nature may result in a breach if the situation is not rectified) or violations (failure to comply with a AML/CTF legal requirement).

Specifically, no cases of ML/TF deficiencies related to unwillingness on the part of entities, but to inaccurate/inadequate implementation, were identified in the supervision process. Some of the causes of these deficiencies are related to the limited availability of AML/CTF specialists in the market, lower level of awareness of money laundering and counter-terrorist financing risks among employees in the territorial units, some deficiencies in their training and workload. The NBR is well aware of the importance of training and awareness, as most of the deficiencies identified in the supervisory actions were linked, in one way or another, to errors by staff involved in the implementation of financial institutions' procedures as a manifestation of operational risk.

In order to mitigate this vulnerability, an obligation for financial institutions to incorporate in their employee training programs both the findings of supervisory work and an awareness component of the consequences of supervisory weaknesses and the potential implications for the institution and those responsible for the occurrence of risks has been included in the sectoral regulation. As a result, institutions should provide ongoing training to those responsible for implementing the measures set out in the KYC rules to ensure that they are aware of the legal requirements, their responsibilities under the KYC rules, the risks to which the institution is exposed according to its own risk assessment, the consequences of not properly fulfilling their responsibilities and the implications for them and the institution should risks arise, and that they have sufficient information to recognize transactions that may be related to money laundering or terrorist financing. Institutions should include in their training program information related to legal requirements, relevant guidelines, their own risk assessments, know-your-customer rules, training information and feedback from the National

Office for the Prevention and Control of Money Laundering, together with relevant practical issues arising from their own and, where appropriate, their group's work, including typologies and case studies. In addition, financial institutions shall periodically check all persons responsible for implementing the measures laid down in the Know Your Customer rules to ensure that they are properly trained to perform their duties. In particular, institutions shall take into account in their control departments, branches or other units and agents and distributors that do not report suspicious transactions subsequently detected by the (central) institution, if suspicious elements have been identified at their level, as well as those for which deficiencies are identified by internal audits or supervisory actions of the National Bank of Romania.

According to the inspectors' findings, although the supervised sector, and in particular the banking sector, understands its obligations, ML/TF risk is present. However, vulnerabilities were identified during the supervisory work and related recommendations or, where appropriate, sanctions were issued. It should be stressed that this is not a general phenomenon, such findings have been observed over the years and are not present in every institution/inspection, so they cannot be considered as a pattern for the financial system supervised by the NBR.

The most frequent violations identified over the years (this does not mean that they are prevalent in the system), based on general or targeted inspection objectives, were related to:

1. Risk assessment:
    - within the internal risk assessment, the European Commission Report / the results of the supranational risk assessment were not taken into account (for example, the products/activities considered in this report as presenting a high risk were classified by the institution as having a standard or low risk);
    - in the risk assessment at customer level, relevant factors that, either individually or consolidated, may increase or decrease the money laundering and terrorist financing risk posed by a business relationship or occasional transaction have not been taken into account (especially in the case of credit/leasing companies);
    - regarding the methodology for classifying clients in the portfolio according to risk, cases of erroneous client classification were identified in the analyzed sample or in the databases (especially in the case of credit/leasing companies);
    - the superficial application of additional measures to know the clientele, without including the specific measures aimed at managing the identified risk; and
    - inadequate/insufficient indicators used in the assessment of compliance risk / AML (especially in the case of lending/leasing companies).

2. Internal controls:
    - inadequate resources allocated to internal control functions (especially in the case of lending/leasing companies);
    - the lack of the most appropriate measures to remedy the deficiencies reported by the internal control functions;
    - failure to assess/report deficiencies in customer awareness/AML/CTF; and
    - deficiencies in training and testing procedures (especially in the case of lending/leasing companies).

3. Governance: The role of the board of directors or senior management
    - allocation of insufficient resources for internal control functions/AML/CTF department; and
    - implementing ineffective measures to remedy deficiencies reported by internal control functions.

4. Customer awareness measures:
    - deficiencies regarding the setting of the parameters of the applications used to identify the PEP/lack of a PEP identification system (especially in the case of credit/leasing companies);
    - failure to apply adequate additional measures to know the clientele for other high-risk categories, distinct from the category of PEP clients (especially in the case of credit/leasing companies);
    - deficiencies in monitoring the business relationship/transactions;
    - cases of non-updating of customer data;
    - numerous procedures with many cross-references, which are difficult to use and not specific enough, too formalized, reproducing legal provisions instead of establishing precise actions adapted to specific people, generating ambiguity in terms of responsibilities; and
    - staff turnover and inadequate training - training is generic, not specific to distinct activities, and lacks an awareness component.
5. Check for unusual transactions:
    - deficiencies in systems or analysis of alerts generated by monitoring applications or analysis of suspicious transactions reported by other organizational structures (Network, Payments, Fraud, etc.) / insufficient number of staff responsible for reviewing alerts;
    - imprecise parameters used for the scenario-based monitoring system, which generates a large number of alerts;
    - the lack of prioritization of the alerts issued by the monitoring systems and the lenient deadlines for their analysis;
    - a poor analysis of the transactional behavior of some customers due to workload/lack of training; and
    - the lack of a control procedure regarding the management of alerts generated by the institutions' IT system.

It should be noted that the above deficiencies have been identified over the years and drastically reduced following recommendations/surveillance measures.

Regarding lending/leasing NBFIs, money laundering deterrence measures (resources, systems) are not as efficient as those of banks (except for non-banking financial institutions that are part of a financial group), but the risk associated with them is also very low.

The deficiencies mentioned or identified above were reflected in the following categories of vulnerabilities:

(i) *Exposure to ML/TF risk in the process of continuous monitoring of customer operations through applications*

In the context of the assessment of the relevant risk factors related to fraudulent transactions, it was found that the ease with which credit institutions offered all customers access to the Internet Banking service (which presents certain inherent ML/TF risks, by

facilitating the rapid and remote ordering of transactions), correlated conduct, mostly, with establishing the achievement of sales targets in the case of employees responsible for attracting customers.

Thus, the access of customers who present a high risk for digital platforms, in the absence of a dynamic process of permanent monitoring of all ongoing operations, which would allow the segmentation of scenarios according to the category of clientele, as well as the possibility of customizing and permanently updating the implemented scenarios/limits for pre- and post-transaction monitoring, reflects a high appetite for the risk of money laundering and terrorist financing, without taking into account the relationship of direct proportionality vis-à-vis the credit institution's ability to manage it.

(ii) *The risk of occasional use of inactive (dormant) accounts for fraudulent transactions.*
The main factor that makes these dormant accounts more prone to fraud is the lack of customer activity. When an account is inactive, either the customer has lost track of the account and is no longer in contact with the bank, in which case the customer will most likely not notice any unauthorized activity on their account, or may raise the suspicion that that customer is waiting the timing of using the account depending on the outcome of unexpected earnings. In both cases, the unusual behavior of the customer in relation to the nature and purpose of the business relationship can be noted.

From the analysis carried out, it was found, among other things, that some of the legal entities that had opened accounts at several banks, ordered some transactions to be carried out after long periods of time in which the only recorded operations consisted in the automatic payment of account management fees, and when these accounts became active, the transactions carried out were predominantly external, unrelated to the object of activity or their value far exceeded the transactional volume declared by the clients at the initiation of business relations.

At the same time, issuing possible alerts was impossible in the absence of detection rules/scenarios that correspond to individual risks (information held about the client), as well as in the impossibility of examining the history of transactions concluded during the business relationship, even more so especially since these accounts were closed shortly after the operations were carried out.

(iii) *Exposure to ML/TF risk in the process of approving the initiation of business relations / account opening, in conjunction with the existence of non-compliant standards of derogation from the application of customer due diligence measures to the initiation of business relations / account opening.*
During the checks carried out on the processes of opening accounts at credit institutions in Romania and used to carry out fraudulent transactions, such as CEO/BEC fraud, the inadequacy of KYC measures, respectively the lack of effective measures in terms of internal control, was found, aspects that led to a flawed assessment of intrinsic risks from a ML/TF perspective, likely to affect the entire process of getting to know the client.

The main risk aspects identified with regard to customer awareness (KYC) measures applied at the time of initiating business relationships were:

- the low level of awareness of the risks of ML/TF at the level of employees within the territorial units, considering that they did not notice the suspicious nature of the initiation of business relations on the same day, at the same territorial unit, with several commercial

companies having the same beneficiary real, as well as objects of activity and identical registered office addresses;

- failure to identify the unusual nature of the transfer of clients' operational activity from one bank to another, after only a few months, given that these entities were recently established commercial companies;
- lack of mandatory information in the account opening files (examples - extracts from the Trade Register, operating authorizations);
- inconsistencies between the object of activity of legal entity clients, according to the constitutive act, and the information provided by the territorial unit in order to approve the initiation of the business relationship;
- the branches (customer relations managers) did not do the necessary due diligence to understand the reason why people domiciled in other states opened accounts at a bank in Romania, without having a solid economic justification for their requests for banking products or services in Romania, without presenting documents issued by the Romanian authorities (example - temporary residence permit), or proof of any connection of these persons with the "suppliers" of social headquarters.

(iv) *ML/TF risk and integrity standards / conflicts of interest*

Institutions must ensure that decisions in the line of prevention and control of money laundering and terrorist financing are taken independently, without being affected by possible influences, pressures or conflicts of interest, meaning that they must define, control and implement an activity management framework that ensures efficient and prudent administration, including by separating the duties between the operational and monitoring functions. From the analyzes carried out so far, it was possible to observe, in several cases, the predilection of the customers in the sample for certain territorial units of credit institutions, which could indicate deficiencies in compliance with integrity standards.

In order to reduce ML/TF risks, institutions must compensate for the potential lack of independence generated by conflicts of interest resulting from the remuneration of staff according to certain commercial performance indicators, stimulated by an inadequate remuneration policy (low salaries), by implementing controls internal measures intended to prevent, in this sense, the impact on the process of classifying clients based on risk, also taking into account the dynamic business environment in which they operate, also characterized by staff turnover.

These are, along with monitoring for the prevention of internal fraud, tools that prevent the exploitation of bank employees for money laundering. The only case presented in the risk assessment is an old case, which involved a very small amount compared to the level of assets in the sector.

(v) *vulnerabilities in ensuring the confidentiality of information held in relation to money laundering and terrorist financing risks* (respectively, requests for information / recommendations made by the central bank regarding the business relations of the reporting entities with certain persons, which have come to the knowledge of the latter).

(vi) *the phenomenon of "de-risking",* respectively the approach characterized by refusal / termination of business relationships to avoid, rather than to manage, money laundering and terrorist financing risks.

Resilience measures/risk mitigation measures

Considering the risk factors mentioned above, the NBR has issued recommendations for the implementation of the following measures to improve the management framework, policies, procedures and controls implemented to mitigate and effectively manage money laundering risks money and terrorist financing:

- not granting or, as the case may be, ceasing the provision of digital banking services, which allow the rapid initiation of fund transfers, to customers included in the categories of high and medium-high risk of money laundering and terrorist financing;
- exercising increased vigilance by implementing additional controls to help reduce the risk of fraud and money laundering and terrorist financing associated with inactive (dormant) accounts;
- the centralization of the approval of the initiation of business relations / the opening of accounts, regardless of the risk associated with them, at the level of a structure within the head office of the institution
  credit of a Romanian legal entity / branch of a foreign legal entity credit institution;
- the elimination of the possibilities / situations of derogation from the application of the provisions of the internal rules regarding knowing the clientele and opening accounts, so as to ensure the compliant application of the provisions of the regulatory framework regarding the prevention and combating of money laundering and the financing of terrorism;
- the implementation of demanding human resources management standards at the level of all structures involved in the processes of preventing money laundering and terrorist financing, through:

    - compliance with appropriate standards for the employment of persons with responsibilities in the application of customer awareness measures;
    - pursuing the improvement of professional skills and awareness of ML/TF risks at the level of all organizational structures with responsibilities within AML/CTF processes, including by presenting the relevant practical aspects resulting from their own activity,

- carrying out internal audit missions to ensure an independent assessment of the effectiveness of conflict-of-interest management policies and the integrity of the employees of the structures involved in customer due diligence processes in order to prevent and combat money laundering and terrorist financing;
- conducting internal audit engagements to provide an independent assessment of how record-keeping procedures and all documents comply with legal requirements, including establishing access to them (strictly on a need-to-know basis), reporting procedures internally and to the competent authorities, including reporting and communication systems and channels, ensure full confidentiality of information requests, as well as data related to the prevention of money laundering and terrorist financing;
- assessing situations where certain risk factors associated with a client arise, including in the process of updating documents and information, which should not automatically lead to the termination of the business relationship; the decision taken should be proportionate to the risk and based on an analysis of the concrete situation, in order to establish, gradually, the necessary measures for the management of related risks, in accordance with the provisions of the relevant legal framework;
- segmentation, customization and updating of scenarios/limits implemented for pre- and post-transaction monitoring, in order to ensure a dynamic process of permanent

monitoring of all operations performed by customers through digital applications (for example, transfer operations performed through the internet banking channel), especially in the case of high-risk customer access to digital platforms, insufficient risk management generated by the use of these digital services may lead to serious violations;

- holding training sessions dedicated to AML/CTF obligations, including the consequences of failure to fulfill responsibilities and the implications for the institution and for the persons who hold such duties through the job description or who is responsible for non-compliance with legal provisions, in case of incidents;
- the assessment of all employees responsible for implementing the measures provided for in the rules on knowing the clientele and those responsible for coordinating the implementation of the internal rules for the implementation of international sanctions for the blocking of funds, to ensure that they are properly prepared for the performance of their duties, from the perspective of ensuring the confidentiality of data and information, as well as to ensure that their obligations regarding the management of confidential information are expressly stated in the job description.

The financial institutions have the obligation to notify the National Bank of Romania of the adopted measures, within the terms established by it.

The NBR is constantly acting to support entities in understanding developments and implications regarding ML/TF risks. The entities supervised by the NBR were actively consulted on the draft law transposing the Directive (Law no. 129/2019) and on the draft regulation of the NBR (NBR Regulation no. 2/2019) and submitted comments/observations regarding the provisions of the law.

Also, with the entry into force of the new legal framework, the NBR organized meetings with the reporting entities (and other than credit institutions), in accordance with the recommendation of the Moneyval Committee in the Detailed Report issued as a result of the fourth assessment round mutual of Romania. The recommendation was to take actions aimed at increasing the awareness of non-banking financial institutions, electronic money issuing institutions and payment institutions regarding their AML/CTF obligations and supervisory authority expectations.

The NBR acts through three distinct channels to enhance and improve the guidance of supervised entities, respectively through:

(i) issuing tailored and highly detailed recommendations for specific/individual entities, based on findings from surveillance activity regarding their system/prevention measures or in response to specific requests for guidance. If necessary, we can provide examples where we have addressed several specific measures to a single credit institution, following the supervisory report.
(ii) issuing specific recommendations/measures for the supervised sector/sub-sector if threats/vulnerabilities of common interest are detected;
(iii) holding meetings/sending letters to industry associations/representative bodies regarding measures involving the need for coordination between supervised entities to achieve best results.

(i) Guidance provided by the NBR for supervised entities through specific documents (measures or recommendations) issued following supervisory actions carried out based on the risk-based approach

One of the strategic objectives assessed by the NBR in each supervisory action planned for 2021 was "to assess the methodology of supervised entities in conducting and updating risk assessment, its implementation and the policies developed to manage and mitigate the risks of money laundering and terrorist financing, and of circumvention of international sanctions, respectively, to which the institution is or could be exposed". As most of the supervisory reports for the 2021 actions are already drafted, the process of issuing very specific actions or recommendations to address the findings is an ongoing one. These types of tools used in the supervisory process are, in the NBR's view, one of the most effective forms of guidance, as the measures are tailored to each institution, adapted to the specific business model, governance structure and internal control system of the supervised entity and to the specific vulnerabilities identified. 40% of the banking sector was covered in 2021 by inspections that included this specific objective (14 credit institutions out of 35). At the level of the other types of entities that are supervised by the NBR (non-bank financial institutions, payment institutions or electronic money issuers), a total of 12 inspections were also carried out that included this specific objective.

(ii) Letters sent by the NBR to the supervised sectors (some of which are related to types of ML/TF, and others to risks/threats)

With regard to the ML/TF typologies, it is important to underline that the NBR is empowered by law only to verify compliance by supervised entities with the provisions of the legal framework on AML/CTF and the implementation of international sanctions, without having, in fact, powers related to the investigation of money laundering/terrorist financing cases/transactions. Also, the NBR is not the competent authority to receive STRs from supervised entities, such tasks being in relation to the NOPCML. Consequently, the guidance on the typologies of ML/TFs that can be developed internally by the NBR is very limited and largely based on information received from other authorities receiving, analyzing or investigating such information/cases and/or from external public sources. However:

1) In 2020 - 2021 the NBR sent over 100 information letters to the financial system (and in some cases they also included requirements to take proportionate measures for risk management), regarding: business relationships in which certain entities are involved associated with money laundering activities, warnings regarding the identification of certain types of suspicious transactions, fraud or attempted fraud, feedback from NOPCML regarding STR reporting, fictitious banks, publication of guidelines/instructions/final reports of the experts, de-risking, international sanctions, etc.
2) During 2020 - 2021, at the highest level, the NBR issued several letters of recommendation, addressed to all institutions under its supervision or to some sub-sectors. E.g:
    a. 2 letters (no. 94/February 20th, 2020 and no.138/March 11th, 2020, supplemented and detailed by letter no. 152/18.03.2020), regarding some types of money laundering. Specific recommendations were ordered for the entire banking system so as to mitigate the risks identified by the NBR following several supervisory inspections.
    b. no. 504/September 10th, 2020 for the entire banking system, regarding the phenomenon of derisking, accompanied by a set of instructions on how to approach this phenomenon.
    c. no. 517/September 15th, 2020 for the entire system supervised by the NBR, regarding the legal provisions regarding the confidentiality of information and

the necessary measures to be taken to comply with the obligations generated by this field.

d. no. 554/October 5th, 2020 regarding the phenomenon of identity theft in order to obtain loans, based on false identity documents;
e. no. 323/May 19th, 2021 - regarding de-risking;
f. no. 589/September 10th, 2021 - recommendations for all credit institutions in relation to the application of international sanctions regimes, etc.

(iii) Training and meetings with the supervised sector

After the entry into force of the NBR Regulation no.2/2019 on the prevention and control of money laundering and terrorist financing, the NBR organized 4 meetings with supervised entities (all credit/leasing NBFIs, PIs, EMIIs supervised by the NBR were invited, with 83% of the sector participating). These consisted of presentations of the new aspects of the legislation and open discussions on issues that could raise implementation issues identified by the NBR and the financial sector. Discussions focused on the requirements for drafting risk assessments. The NBR representatives provided explanations of supervisory expectations and examples of possible sources of information, at European and national level, that could be used for entities' own assessments. Practical examples were also given of approaches for processing the possible transactions they may face, to reflect the specific risk taken by each entity in relation to its activities.

The sessions were highly appreciated by the financial sector. The participants followed the supervisory authority's recommendation to organize within their own institutions a working group dedicated to AML/CTF aspects.

Also, for credit institutions, in addition to the periodic meetings within the committee of compliance officers (which are organized at the request of the Romanian Banks Association), meetings were held through remote communication means, which covered a wide field of compliance, including measures to be implemented to improve the governance framework, policies, procedures and controls to effectively mitigate and manage the risks of money laundering and terrorist financing.

Money laundering typologies, whenever notified/identified, were also disseminated to supervised entities[17]. As a result of cooperation with other institutions and authorities in the AML/CTF area, the NBR has identified a number of downstream risks in relation to certain individuals and legal entities. Thus, in order to assist reporting entities in the process of complying with the relevant legal framework, to be able to continuously assess their business relationships with their customers and, in particular, to be able to identify and report suspicious transactions and activities through suspicious transaction reports, the central bank has sent letters to the supervised financial system outlining possible ML/TF threats whenever they arise in relation to possible business relationships with certain natural and legal persons.

The Central Bank Supervision Directorate closely monitors all developments in this area, participates in EU working groups and supervisory colleges and implements best

[17]According to MONEYVAL, the 4th Round of mutual assessments, the second compliance report presented by Romania in 2019, „Furthermore, the definite increase in the number of sanctions led to a corresponding increase in the number of RTSs. The sector supervised by the NBR and especially the banking system has an overwhelming share in the total number of STRs. (85.57% of the total number of STRs)". As a result, an official letter was received from NOPCML expressing high appreciation for the direct contribution of the NBR to the continuous increase in the number of STRs.

requirements and practices. Reporting entities supervised by the central bank are aware that if they want to be part of the single financial market and be competitive, they need to align with legislative and regulatory developments in the market. In order to understand the NBR's approach to supervision along the AML/CTF line on the obligation for entities to identify and assess money laundering and terrorist financing risks, we will briefly outline the evolution of the legal framework on this issue and how the conclusions resulting from supervisory work contribute to the architecture of the new regulatory framework.

Under the legislation, institutions have been required to conduct their own risk assessments to identify and assess the risk of money laundering and terrorist financing at the client level, at the level of services and products offered, and at the level of the whole business, taking into account national and sectoral assessments available in the jurisdictions in which they operate and assessments at the level of the group to which they belong.

At the beginning of 2020, at the request of the NBR, all credit institutions made their own risk-based assessments available to the central bank. At the same time, on-site surveillance activities were also aimed at assessing the supervised entities' understanding of vulnerabilities, and therefore more attention was paid to internal risk assessments. All these aspects are analyzed either during on-site inspections or continuously in off-site monitoring activities. Based on all these aspects, the main recent priorities in surveillance activity have been:

- The assessment of the methodology for carrying out and updating the risk assessment, implemented by the supervised institutions, of the way of its implementation and, respectively, of the policies developed for the management and reduction of the risk of money laundering and financing of terrorism and evasion of international sanctions to which the institution is or could be exposed;
- Assessment of how the recommendations sent to the sector during the previous year were implemented;
- Assessment and implementation of digitization strategies and their impact on business models and implications for internal governance and internal control system (establishing a healthy and effective governance culture of ML/TF risks associated with the implementation of digitization strategies, adoption of FinTech solutions/ new technologies, the increase in cybercrime during the pandemic and the weaknesses of the IT systems used in the know-your-customer process, the prevention of money laundering and of terrorism financing and a robust internal control system, in particular from the perspective of risk assessment, correct identification of customers and the quality of the data collected at the time of the initiation of the business relationship, the measures to know the customers and to monitor the transactions);
- Assessing the ML/TF risks associated with digitization projects to allow access to both individuals and legal entities, and to provide digital services and solutions;
- ML/TF risks generated by reliance on digital and remote solutions to conduct day-to-day operations and provide services to clients;
- Collaboration with supervised institutions, NOPCML and judicial bodies to identify and raise awareness of emerging risks, namely new types of ML/TF, in the context of a potential new economic crisis and to update risk assessments accordingly.

The review of the supervised sector also confirmed the general trend towards a cultural change in the banking sector. Digitization and acceleration of banking processes and workflows positions banks to new challenges, including in the prevention of ML/TF. Shorter processing times and faster processing of payments, especially instant payments, together with certain forms of online transactions and new payment methods pose a threat to the

application of adequate preventive measures. Also, in this context, new risks are manifested as a result of innovative business models and new technologies of FinTech companies.

It should also be mentioned that innovative technologies can also offer opportunities in terms of managing money laundering and terrorist financing risks. Potential areas of application in this regard could include STR monitoring and processing. Better algorithms could be used to generate fewer false-positive alerts, enable fast and real-time processing, and thus ensure more effective monitoring and reporting of suspicious transactions. However, according to the banks, fully market-ready solutions are not yet available.

For most banks, it is not very clear how specific cases of terrorist financing can be identified in the ex-ante assessment of transactions, the key measure being to compare customer lists with published international sanctions lists or to detect certain anomalies.

The changes in the regulatory framework and supervisory practices of AML/CTF at EU level have also been reflected in the supervisory process in Romania, with the implementation of a risk-based approach[18] in the assessment of supervised institutions, as already presented in this Report. Supervisory powers and tools. Thus, the amount of information requested, the frequency and intensity of checks, analyses and assessments take into account the nature of the activity, correlated with the level of money laundering and terrorist financing risks identified at individual, sectoral or national level. This risk-based approach procedure governs the processes, mechanisms and practical arrangements that enable the NBR to exercise its supervisory powers in the area of prevention of money laundering and terrorist financing in a manner proportionate to the money laundering/terrorist financing risks identified at the level of the supervised institutions.

The Money Laundering and Terrorist Financing Prevention and International Sanctions Unit collects relevant and reliable information in order to obtain an adequate understanding of the risk factors faced by the subjects of the assessment. For this purpose, relevant data and information shall be collected:

- international, national and sectoral risk assessments;
- reports/information issued by NOPCML and other national and international authorities/institutions with competence in the matter (e.g. EBA);
- the exchange such information with other competent authorities, at national level or abroad, holding relevant information on the matter, including those involved in the supervision of firms operating across borders in accordance with the ESA Joint Guidance on cooperation and exchange of information for the purposes of Directive (EU) 2015/849 between competent authorities supervising credit and financial institutions, obtained through participation in supervisory colleges or through bilateral cooperation;
- reports on the financial situation/stability from a microprudential and macroprudential perspective;
- information/questionnaires, rules, situations, reports and reports submitted by institutions, analyzed within the off-site supervision processes, the changes that occurred in the situation of the supervised entities in the period between the conclusion of the on-site supervision action and the drafting of the final documents, which are included in individual files of supervised entities;

[18] In 2017, the NBR approved and implemented the Procedure on the process of risk-based supervision and assessment of credit institutions, non-bank financial institutions, payment institutions and institutions issuing electronic money, based on their exposure to the risk of money laundering, terrorist financing and non-implementation of international sanctions. The procedure has subsequently been updated 5 times.

- findings resulting from on-site inspection actions, off-site and/or on-site surveillance reports or off-site assessments/analyses;
- the exchange of information with the prudential supervision services, which is carried out by means of supervision reports and the ad hoc exchange of information whenever there are reasons for a specialized analysis in the field of preventing money laundering and terrorist financing;
- the lists of international sanctions provided by the competent international bodies, respectively the UN Security Council and the EU.

Other sources of information are also considered, such as:

- information and analysis provided by professional associations, institutions/economic agents active in the financial sector or in related sectors, such as typologies and information on emerging risks;
- information from international standard-setting bodies, such as mutual assessments of the actions taken by the Member States in relation to preventing and combating money laundering and the financing of terrorism, the anti-corruption system and the tax regime;
- sources of public information, such as studies/reports/articles published in the press; whistleblower reports, i.e. information informally submitted to the supervisor by employees of entities, in accordance with Article 61 of Directive 2015/849 and the law in the field of preventing and combating money laundering and terrorist financing transposing the Directive.
  In the case of all financial institutions supervised by the NBR, the relevant information shall include at least: the ownership structure and governance structure of the company, taking into account whether the subject of the assessment is an international, foreign or domestic institution, a parent company, a branch, a subsidiary or other form of incorporation, and the degree of complexity and transparency of its organization and structure;
- the reputation and integrity of executives, members of the governing body and significant shareholders;
- the nature and complexity of the products and services offered, as well as the activities and transactions carried out;
- the distribution channels used, including the free provision of services and the use of agents or intermediaries;
- the types of clients served;
- the geographical area where the activities took place, in particular if they were carried out in high-risk third countries, as well as, where applicable, the countries of origin or establishment of a significant part of the customers and the countries that are subject to international sanctions imposed by the UN and the EU;
- the quality of internal governance mechanisms and structures, including the adequacy and effectiveness of internal audit and compliance functions, the level of compliance with legal and regulatory requirements for the prevention of money laundering and the financing of terrorism and the enforcement of international sanctions, as well as the effectiveness of policies and procedures in the field of preventing and combating money laundering and terrorist financing, to the extent that they are already determined;
- information from prudential supervisors regarding any suspicion of committing or attempting to commit money laundering or terrorist financing crimes, as well as regarding any other finding that indicates a possible violation of the regulatory

framework on preventing and combating money laundering, and of terrorist financing or internal control deficiencies that may be relevant.
- information on changes to an institution's activity or business model that could expose institutions to an increased risk of money laundering or front-loading.
- the prevailing "corporate culture", in particular the "culture of compliance" and the culture of transparency and trust in relations with the competent authorities;
- other prudential and general aspects, such as years of operation, liquidity or capital adequacy, alignment of policies and procedures in the field of preventing and combating money laundering and terrorist financing with the specific requirements of the EBA Guide on credit origination and monitoring - EBA/GL/ 2020/06.

The assessment of each of these categories of data mentioned above is carried out based on the criteria provided in the specific procedure.

The Money Laundering and Terrorist Financing Prevention and International Sanctions Enforcement Unit shall assess the extent to which the identified inherent risk factors affect the risk profile of the entity or group of entities and the extent to which the systems and controls in the area of preventing and combating money laundering and terrorist financing implemented by the assessed legal person are adequate to effectively mitigate the inherent money laundering and terrorist financing risks to which it is exposed, thereby determining the level of residual risk.

In order to assess the risk profile of money laundering/terrorist financing and non-application of international sanctions, respectively the type and level of risk that is maintained even after the actions to reduce it, the surveillance actions analyze at least the following components:

1) Risks arising from the business model, size, nature, volume and complexity of the institution's activities:
- the business model;
- the size of the institution;
- the geographical area in which it operates;
- the nature and complexity of the product and service portfolio;
- customer profile;
- distribution channels used;
- prudential and general aspects, such as elements of credit risk, elements of operational risk, developments recorded by prudential indicators that may constitute ML/TF risk generating factors, depending on the case.

2) The risks arising from internal governance and the internal control system, at the level of international sanctions enforcement activities, prevention of money laundering and terrorist financing:
- the nature, structure and reputation of the shareholding;
- the reputation and integrity of members of the governing body and middle managers;
- the complexity and transparency of the organizational structure;
- the way of assigning duties and responsibilities at the level of positions/functions;
- the way of exercising the duties and responsibilities by the personnel/management structures involved in AML/CTF activity and applying international sanctions;
- the existence of effective communication and reporting channels;
- the existence of appropriate policies and procedures, as well as formalized processes;
- the degree of adequacy of human resources engaged in AML/CTF activity and the application of international sanctions;

- the corporate culture, the relationship with the authorities with responsibilities in the field of AML/CTF and enforcement of international sanctions;
- the existence of a solid internal control framework regarding AML/CTF activities and the application of international sanctions (the management of ML/TF risks and the non-application of international sanctions, the efficiency of the compliance and internal audit functions).

3) The risks arising from the way of applying the provisions of the legal framework in force in the matter of ML/TF:

How the institution defines, identifies and manages Publicly Exposed Persons (PEPs);

- The way in which the institution defines and ensures the identification of the real beneficiary;
- Assessment of procedures and processes for the application of standard, simplified and additional measures;
- The way in which the institution evaluates and classifies the clientele and transactions according to the degree of potential risk associated with them;
- The way in which the institution manages the risk associated with customers and transactions presenting a potentially higher degree of risk;
- Assessment of procedures and processes for identification, management and notification of operations likely to have the purpose of money laundering or terrorist financing;
- Assessment of the procedures and processes applied for the identification and reporting of transactions carried out with amounts in cash, in lei or in foreign currency, and of external transactions whose minimum limit represents the equivalent of EUR 10,000;
- How to update and manage the documents used to identify customers, respectively the secondary records and the registration of financial operations carried out by customers.

4) The risks arising from the implementation of international sanctions:

- analysis of the reports sent to NAFA and NBR regarding the designated persons and/or entities, identified as a result of the application of customer awareness measures, according to the reporting mechanism and model;
- analyze proceeding implemented for update lists of designated persons/entities;
- the analysis, as the case may be, of authorizations, exemptions, notifications of transfers on certain relationships that are subject to international sanctions, if applicable;
- testing compliance with the provisions of the Sectoral Regulation of the National Bank of Romania, respectively verifying whether the supervised institution has adopted and submitted to the NBR the internal rules for the implementation of international funds blocking sanctions, which include at least:
  - procedures for detecting designated persons/entities;
  - the duties of the persons responsible for applying the relevant legislation in the field;
  - the internal reporting procedures regarding the identification of a designated person/entity;
- analysis of how to manage alerts, in case all the identification elements of the designated person/entity do not match.

After evaluating the components mentioned above (some of them may not be taken into account in the supervisory actions, depending on the specifics of each entity/cluster), a rating between 1 and 4 is assigned to each component. The rating for each element is determined by combining two determining factors, namely the rating for the inherent risk factors and the rating for the factors that mitigate the inherent risk of ML/TF and the risk derived from the non-application of international sanctions, and by taking into account:

- the probability that the risk will materialize, respectively materialize in transactions/operations involving the abusive use of the banking/financial sector to channel funds of illegal or even legal origin for money laundering and terrorist financing purposes;
- the estimated impact on the integrity, good functioning, reputation and, implicitly, on the stability of the institution;
- the existence of policies, controls and procedures that adequately manage the risks of money laundering and terrorist financing identified at national level, at EU level, within the member states in which they operate and by the obliged entities. These policies, controls and procedures must be proportionate to the nature and size of the respective obliged entities.

The overall score, which reflects the residual risk (relative to the sector/sub-sector to which the entity belongs), is determined as a weighted average of the ratings of the above-mentioned evaluated components. However, these ratings allow the supervisor to determine whether a financial institution's level of ML/TF risk has resulted from, for example, a high level of inherent ML/TF risk and effective anti-money laundering controls /terrorist financing or from a moderate level of money laundering/terrorist financing risk and ineffective anti-money laundering/terrorist financing controls.
All these activities and analyzes enable better resilience of the sector to inherent threats.

4.2.2. Conclusions regarding individual sub-sectors

1. The bank sector

The banks, most of which belong to international groups (but all with an EEA-based parent company and no owner/controller risks), offer both individuals and businesses a full range of banking products and services, including deposits, current accounts, loans, transfers, currency exchanges, safe deposit boxes, etc.

The banking sector has a growing inclusion rate, in most cases it is, in the case of natural persons, resident customers who maintain a long-term relationship with the credit institution for primary use, namely saving, collecting salaries/pensions through online payment and, where applicable, mortgages. The use of financial services in Romania is low, especially in the rural / elderly sector. In fact, international statistics show that Romania has one of the lowest levels of financial inclusion among countries in the region. A relatively large number of people who have accounts with credit institutions use financial services to a low degree, using their accounts with credit institutions only to cash in some amounts (e.g. salaries, pensions, scholarships), while other transactions are carried out in cash and money is withdrawn immediately from ATMs. However, lately, especially in order to attract young people, there has been a noticeable trend to launch products based on initiating a business relationship without physical presence or through agents, accelerated by the COVID-19 pandemic and the increased use of online purchases. The Romanian banking system is characterized by the existence of a dense network of banking centers and both online and

mobile banking facilities are available. The number of branches is decreasing, but this is a general trend in the EU.

According to statistics[19] published by the European Banking Federation, Romania is the country with the highest number of inhabitants per bank employee, namely 365 inhabitants per bank employee (while, for example, Luxembourg has the lowest number, with only 23 inhabitants per bank employee). The average number of inhabitants per bank branch, 4,781, is also above the EU average (3,281). This pressure of high customer/bank staff numbers has been reflected in supervisory reports as a vulnerability that sometimes leads to non-compliance with legal requirements in the form of a tick box exercise without due attention to the implementation of the very measures for which the processes were designed (tick box exercise), or to alerts being closed without proper analysis.

Retail and business banks make up the bulk of the market and are representative for this assessment. The banking sector is inherently vulnerable to money laundering and terrorist financing risks due to a number of factors, such as the large number of customers, the increased speed of transactions and the large volume of financial flows which, according to the general understanding of global money laundering practices, could facilitate the concealment of illegal transactions. Savings and loan banks in the housing sector (2) and credit unions (1) have a much lower inherent risk due to their specific customer base and the fact that many features of retail banking do not correspond to them and also given their small number, market share and unique characteristics (however, they are subject to supervision and individual risk assessment.

As far as the private banking sector is concerned, in Romania it is in fact in most cases only a product name, a marketing strategy used to attract customers, but without the characteristics of real private banking in the sense of activity considered high risk from the AML perspective (defined as the provision of personalized services to higher net-worth customers, with a relationship manager acting as a link between the customer and the bank and facilitating the customer's use of the bank's financial services and products. Information on the private banking segment is requested through the annual NBR questionnaire. For example, in 2020 data on the number of private banking customers and transactional volumes (debit/credit) were requested, but the data collected reveals a very limited transactional share. According to the 2020 annual questionnaire data, as of 30.06.2020, there were 7 banks offering private banking services with a total of less than 0.01% of the total customers falling into this category (as mentioned, most of them are actually called private banking but do not fall under the established definition of private banking). Also, their share in transactional volumes, in terms of value of transactions in the first half of 2020, was very low (less than 0.5% of total volumes for other clients). As mentioned, the criteria for classifying clients in the private banking category do not always imply the use of standards similar to those used in other Member States. For example, one bank (which had about 18% of the total number of private banking clients in the whole system) classified as a "private banking client" any client with either assets under management of more than €50,000 or income of more than €2,000/month and, although clients were classified as private banking on the

[19] https://www.ebf.eu/facts-and-figures/structures-of-the-banking-section/

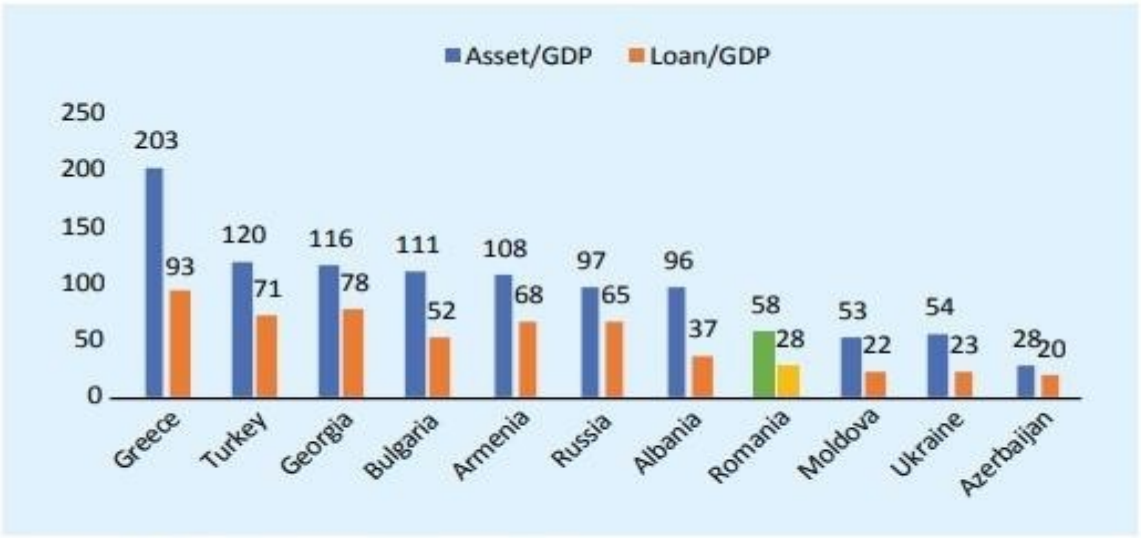
basis of these criteria, they could access the same products as standard clients, the difference being in the quality of service (e.g. a dedicated territorial unit, shorter service time,etc.).

	TOTAL		
	2018	2019	S1 2020
Număr total clienți in perioada de referinta (inclusiv clienti inchisi pe parcursul intervalului de referinta)	23,175,445	23,441,680	22,250,693
Rulaj creditor (echiv EUR)	1,286,767,950,880	1,605,377,403,695	879,008,939,620
Rulaj debitor (echiv EUR)	1,364,585,813,433	1,594,496,612,445	882,822,489,745
Număr*** clienți private banking	14,052	15,891	18,234
Rulaj debitor*** clienți private banking în anul/semestrul de referință (echiv EUR*)	6,951,302,443	5,691,636,580	3,884,423,157
Rulaj creditor*** clienți private banking în anul/semestrul de referință (echiv EUR*)	7,459,958,725	5,788,082,362	4,051,261,817
%clienti private banking	0.061%	0.068%	0.082%
% rulaj creditor clienți private banking	0.580%	0.361%	0.461%
% rulaj debitor clienți private banking	0.509%	0.357%	0.440%

However, with regard to the risk associated with private banking activity, we note that during each on-site supervisory inspection all private banking clients were requested to provide a statement containing at least their name, personal identification number, assigned risk, business relationship start dates, most recently updating information, country of origin/residence/citizenship, source of funds, volume of transactions during the period analyzed (debit/credit), volume of cross-border transactions within the EU, volume of cross-border transactions outside the EU, loans granted during the period analyzed (date of disbursement, amount, currency, type of credit, type of guarantee, credit balance at reporting date), volume of deposits, products held. Based on these reports, the inspection sample under review also includes private banking clients. The enhanced customer awareness measures applied to this type of customer, the internal control system applicable to private banking customer processes, etc. are also analyzed and, where appropriate, recommendations or measures are issued based on the inspection findings.

As far as cryptocurrencies are concerned, it should be mentioned that the NBR has been carefully monitoring and taking a position since the beginning of these activities in Romania. Since March 2015, the NBR has issued a series of public statements highlighting the risks.

The number of banks and the volume of assets are small compared to the major financial systems in the EU, as well as compared to a number of states in the region.



Source: National Bank of Romania

Cash

The analysis showed that money laundering and terrorist financing still frequently rely on the use of cash. As a result, cash transactions are a regular subject of suspicious transaction reports and investigations in the banking sector, as well as in other sectors.

Operațiuni bancare cu numerar				
	2017	2018	2019	2020
Numărul de conturi deținute de persoanele fizice	19,783,515	23,546,394	24,433,561	24,681,152
Volumul conturilor deținute de persoanele fizice (mil EUR)	16,877.5475	23,036.2293	28,072.7325	36,619.2324
Volumul de depozite deținute la vedere de persoanele fizice (mil EUR)	9,062.6117	10,821.0896	11,487.6512	10,897.4035
Volumul de retrageri în numerar ale persoanelor fizice (mil EUR)	34,246.7579	39,876.8566	46,422.4279	43,735.5001

Persoane juridice					
Numărul de afaceri gestionate de bănci cu operațiuni în numerar	2,179,111	2,216,519	2,549,629	2,384,835	
Volumul total al încasărilor de numerar în conturile persoanelor juridice (afaceri cu licență/fără licență) (mil EUR)	47,709.7777	50,995.9880	103,604.0926	50,936.4459	
Volumul încasărilor de numerar în conturile persoanelor juridice pentru vânzările de produse cu amănuntul (mil EUR)	17,183.0150	18,774.8217	20,796.8251	18,959.0452	
Volumul încasărilor de numerar în conturile persoanelor juridice pentru servicile cu amănuntul (mil EUR)	2,266.5829	2,514.4043	2,899.1206	2,672.6080	
Volumul încasărilor de numerar pentru vânzările imobiliare către persoane fizice (mil EUR)	323.7675	331.9124	361.2454	270.6031	
Volumul încasărilor de numerar de la cazinouri (mil EUR)	833.9575	978.7218	1,221.5061	671.2944	
Volumul de numerar pus la dispoziția birourilor de amanet (mil EUR)	288.1366	360.1147	411.2772	314.5822	
Alte încasări de numerar ale băncilor (mil EUR)	4,060.9077	4,386.9371	5,181.6218	4,488.0948	An fost avute în vedere încasările/plățile în numerar în/din conturile persoanelor juridice care desfășoară activități în domenii considerate cu pezentând un risc ridicat de către bănci, conform procedurilor interne.
Alte plăți de numerar ale băncilor (mil EUR)	2,870.9189	3,615.9672	4,670.3679	4,369.1796	

Regarding the risk associated with the intensive use of cash, in addition to the obligation[20] existing reporting, we mention the following measures to reduce it taken by the NBR:

1. The list of documents requested before the inspection action includes the databases used by the inspection team to select samples of cash/customer transactions and to assess the effectiveness of statistical reporting to NOPCML:
    - The Database of occasional transactions carried out during the period analyzed (this will contain information such as: date of transaction, customer name, unique personal identification code, type of transaction, amount, currency sold/purchased or paid/received, beneficiary/payer and their country in the case of money remittances).
    - List of customers who have carried out cash transactions during the period analyzed (which is usually at least one year). The list contains at least the following information: customer name, unique identifier, type of customer (legal entity/individual), country of origin, country of residence, nationality, date of opening of the relationship, risk category, number of STRs issued in relation to the customer, number of requests for information from the authorities in the case of a PEP or private banking customer, number of cash withdrawals and total amount during the period analyzed, number of cash deposits and total amount during the period analyzed, number of alerts from transaction monitoring applications during the period analyzed.
    - Reports submitted during the period under review to the NOPCML for cash transactions, in RON or in foreign currency, equal to or greater than the RON equivalent of EUR 10,000, including transactions that appear to be linked to each other.

The following aspects should also be mentioned:

Some credit institutions on the Romanian market have decided to reduce the number of units that operate with cash or even to suppress this type of service:

- due to the COVID-19 pandemic, a change in customer behavior has been observed, with a large number of them migrating to using mainly distribution channels such as ATMs or MFMs (multi-functional machines) and payments online/with card;

Through the 2020 questionnaire, the NBR collected a series of relevant data on the issue, such as:

- The number of clients whose operating limits via the card have been increased above the standard limits;
- The number of customers whose internet banking or mobile banking operating limits have been increased beyond the standard limits;

[20]According to Article 7 of the AML/CTF Law (no. 129/2019), reporting entities are required to report to the NOPCML all cash transactions, in RON or in foreign currency, equal to or exceeding the RON equivalent of EUR 10,000, including transactions that appear to be linked*. For money remittance activity, reporting entities are required to submit to the NOPCML reports on transfers of funds with a minimum limit of RON equivalent of EUR 2,000. The reports for these transactions must be submitted to the NOPCML no later than 3 working days from the time of the transaction.
(*transactions that appear to be linked are transactions where the total amount is fragmented into several amounts less than the RON equivalent of the amounts referred to in Article 7 of Law 129/2019, also having common elements such as: the parties to the transactions, including the beneficial owners, the nature or category of the transactions and the amounts involved).
Also in force is Law no. 70/2015, aimed at strengthening financial discipline on cash receipts and payments.

- If the implemented monitoring system detects situations in which a customer carries out several transactions that have a value immediately below the reporting thresholds;
- Ante-factum and post-factum monitoring scenarios (including cash and casual transaction monitoring scenarios).

Credit institutions consider the ML/TF risk associated with cash-intensive behavior as follows:

- Among the criteria used to assess the risk of customers, it is taken into account whether the customer or its actual beneficiary is associated with a sector that uses cash intensively; in some cases, the client's ML/TF risk assessment takes into account the volume and/or number of cash transactions (estimated or executed);
- Institutions have implemented dedicated scenarios for monitoring cash transactions, based on indicators and analyses, such as:

  - account receipts are withdrawn in cash above a certain percentage of the turnover;
  - the number/volume of cash transactions exceeds certain limits (fixed thresholds or deviations from the client's previous behavior);
  - cash withdrawals/deposits made by the same customer at different units of the same credit institution in a short period of time;
  - the declared intention to deposit a large amount of cash by a person unrelated to the customer's account (for example, legal representative, proxy, etc.);
  - *smurfing* (structuring of large amounts of cash into several transactions of small value);
  - frequent cash deposits/bank transfers followed shortly by cash withdrawals;
  - substantial transfers of funds from the company's accounts to the account of the actual beneficiary, followed by cash withdrawals and cash deposits on the same day or at short time intervals, back to the accounts of the ordering company, so that, through the circuit created, the original ordering party becomes the final beneficiary of amounts transferred through accounts;
  - repeated deposits/withdrawals of cash, of the same value, or to/from similar accounts;
  - substantial cash deposits from various individuals, within a short period of time, followed by the immediate cash withdrawal of these amounts;
  - more cash transactions below the reporting threshold;
  - repeated money remittance transactions carried out by the same customer, to different individuals/jurisdictions; high service activity (ATM transactions exceeding thresholds); * consistent cash deposits followed by transfers abroad; * quick movement of funds - from cash to international transfer (cash deposit followed by immediate external transfers); a fast movement of funds - from international transfer to cash (cash withdrawal immediately after external collection of funds); a rapid circulation of funds - from cash to cash;
  - significant cash transactions of customers who do not have a historical (behavior) in relation to the institution (new customers); * large cash

transactions for high risk industries/activities; withdrawing large amounts of cash from inactive (dormant) accounts after recording large collections.

Thresholds can be differentiated taking into account aspects such as the assigned risk category, whether or not the respective customer is a publicly exposed person (PEP), the customer's business segment, etc.

It should be noted that the NBR requires banks to periodically review the scenarios implemented in the applications used to monitor transactions, to carry out an in-depth analysis regarding the establishment of (alert) thresholds and to adapt them taking into account the risk factors arising from their own business models (customer portfolio, completed transactions, etc.). The formalized analysis carried out regarding the accuracy, efficiency and adequacy of the scenarios as a whole, as well as for each customization/modification of the parameters, are also evaluated by the NBR, at least at the time of the inspection action (general on-site inspection – on-site- or thematic inspection, when the objectives of the action include issues related to, for example, IT systems, suspicious transactions, etc.).

2. Examples of recommendations/measures imposed by the NBR on credit institutions, regarding processes aimed at the use of cash:
    - To implement flows and procedures regarding the obligation to carry out an appropriate analysis from the ML/TF perspective of requests received regarding the increase of daily trading limits, in the case of operations carried out through alternative channels, including the need to establish appropriate limits and the periods for which grant the increase;
    - To implement control procedures regarding decisions to approve requests to increase the standard trading limits for operations carried out through alternative channels;
    - Reviewing the AML/CTF customer awareness framework to ensure that:
        - the operational flow implemented to monitor ATM cash deposit transactions is properly formalized to ensure the application of appropriate KYC measures in relation to customer/service risk; and
        - establishing daily transaction limits for ATM cash deposits to reduce ML risk associated with this service;
    - Ensuring the application of the additional measure of obtaining approval at a higher hierarchical level for transactions carried out through the accounts of "high risk" customers, including PEPs, exceeding the threshold of EUR 10,000 or equivalent/transaction, regardless of whether the transactions are carried out in cash or by transfers internal or external;
    - Revising the control methodology in terms of providing the NOPCML with accurate and complete data on cash transactions by establishing a wider range of sampling criteria and alternating these criteria at the time of controls;
    - Carrying out an internal audit mission with the objective of verifying that reports submitted to NOPCML on cash transactions of at least EUR 10,000 or equivalent (including transactions that appear to be linked) contain accurate and complete data, as well as the effectiveness of procedures, processes and IT systems implemented for data extraction and processing.

Financial flows

Another key factor is the business of money remittance services, carried out through banks and involving higher risks, especially in the case of cash transactions of an international dimension (followed by transfers abroad) and payments made outside a relationship of existing businesses.

However, in terms of cross-border transactions with all jurisdictions, less than 50% of the banking sector (15 banks out of 35) was involved in money remittance service activities in 2020, and the amounts represented barely 0 .03% of the total volume of assets employed by the sector.

However, the risk associated with cross-border exposure remains relevant, but not as important as in the case of Member States known to be international financial centers.

In 2020, 7 Romanian banks (including 2 branches of credit institutions from other member states) out of the 31 credit institutions that managed such transactions, had the most intense activity in this sector in terms of the volume of cross-border transactions ordered/collected by customers. These are actually the biggest banks in Romania, covering 60% of the market share.

The most important risk factors related to cross-border operations are represented by the geographical areas and the customers involved in the transaction chain. However, the prevalence of volumes circulated through the same large banks mentioned previously was observed, which is explainable considering their international recognition and the range of services they offer, having a greater financial and IT expertise capacity (special hubs with hundreds of employees monitoring and managing risks).

With regard to geographical areas, namely third countries with high risk and strategic deficiencies[21] (HRTC), the total volume of transactions involving these jurisdictions carried out by banks in 2020 represents 2.39% in the case of recorded receipts and 6.46% in the case of payments made. For this estimate, the NBR included in the HRTC category, the jurisdictions that were included on the FATF list in 2021, although at the time of the operations, in 2020, they were not all on the FATF list of monitored jurisdictions, thus, the estimated volume being smaller. In the context where, for adequate risk management, the legislation requires additional measures to know the clientele in such cases, in order to process some transactions with the jurisdictions in question, the bank requests additional information and supporting documents.

With regard to the customers who made cross-border transactions, respectively regarding the volumes of external transactions recorded on the accounts of customers identified as publicly exposed persons (PEP), 0.37% of these were made through the accounts of resident PEP customers, and 0. 57% through the accounts of non-resident PEP clients [noting that the total number of current accounts held by non-resident clients (individuals and legal entities) was calculated regardless of their currency and the number of accounts held by the same client].

[21]Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries that have strategic deficiencies, as amended and supplemented: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A02016R1675-20210207 - FATF List of High Risk Jurisdictions Subject to a Request for Action: http://www.fatfgafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-forum-act-February-2020.html - FATF List of Jurisdictions Under Enhanced Monitoring – 21 February 2020: http://www.fatfgafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-february-2020.html
- FATF List of Jurisdictions Under Enhanced Monitoring - June 202170: http://www.fatf-gafi.org/publications/high-risk-andother-monitored-jurisdictions/documents/increased-monitoring-young-2021.html

Although the likelihood of a particular customer, type of transaction or product being used for money laundering or terrorist financing is low (as evidenced by the very small number of money laundering cases – many of which are triggered by STRs (banks, as mentioned, have the highest reporting rate and the best prevention systems in place), the total volume recorded presents a challenge for detecting suspicious transactions.

Romania's economy is interconnected internationally and, being a member of the European single market, the free movement of capital applies. Accordingly, the risk assessment must attach great importance to the cross-border threat of money laundering and terrorist financing and assess it as a priority. With regard to cross-border transactions processed by Romania with other countries selected on the basis of a series of criteria, which include, in particular, all neighboring states of Romania, countries where a relatively large number of Romanians live, jurisdictions of particular economic importance for Romania and, of course, the countries that are frequently related, at an international level, to money laundering/terrorist financing activities.

Financial institutions in Romania have a very limited presence abroad, more precisely in only two countries, the Republic of Moldova and Italy. As regards the Republic of Moldova, joint inspections were carried out in accordance with the provisions of the Agreement of Understanding on Banking Supervision of July 27th, 2001 between the NBR and the National Bank of Moldova. The Agreement was recently replaced by the Understanding Agreement, signed on June 11th, 2021, which extends cooperation between the two authorities also in the segment of institutional capacity building in areas such as banking supervision, including the activity of payment service providers and electronic money issuers, financial market infrastructures, cash transactions, prevention of money laundering and terrorist financing, etc., with a view to promoting the smooth functioning of the financial and banking systems. Similarly, on December 12th, 2002, a Memorandum of Understanding was signed between the National Bank of Italy and the NBR on cooperation in the field of banking supervision.

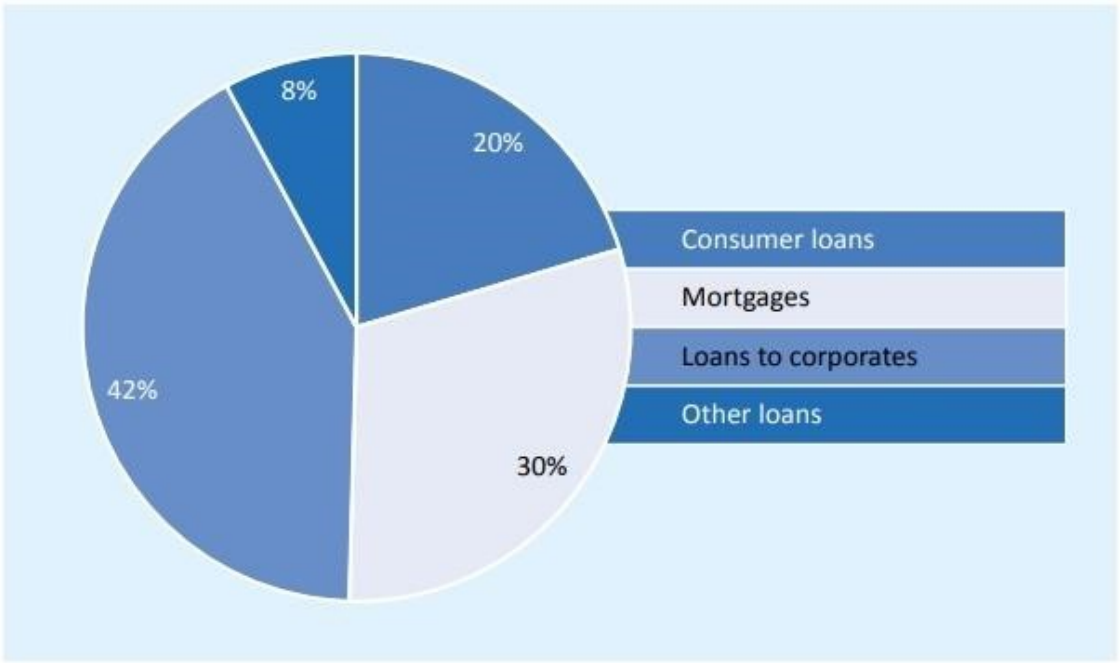
In the context of the identification of serious violations of anti-money laundering rules, in accordance with the ESA's Common Guidelines on cooperation and exchange of information within the meaning of Directive (EU) No. 2015/849 between the competent authorities that supervise credit institutions and financial institutions, the representatives of the National Bank of Romania participate in the supervisory boards in the field of preventing and combating money laundering and terrorist financing of the competent authorities that supervise credit institutions, lending/leasing NBFIs, PIs and EMIIs.

In the case of the banking system, the NBR estimates that the greatest exogenous risks arise from multiple external receipts from different, apparently unrelated originators, transactions that are not consistent with the customer profile and, above all, from the use of so-called trade-based money laundering - a method characterized by payments for complex, fictitious or overstated commercial transactions for which supporting documents are presented. In addition, these are often carried out through several financial institutions, so that each of them has only a partial view of the parties involved in the transactions. All these aspects make it very difficult or impossible to detect money laundering operations of this type under normal conditions.
Regarding identified and identifiable threats, there is a high degree of concern, represented by the fact that the percentage of STRs transmitted by banks (for transactions/activities or attempted transactions) of the national total of STRs is a significant one. At the same time it should be noted that, among all reporting entities, banks have the most developed and

efficient departments, as well as specialized tools. However, the risk remains due to the weight and complexity of financial services offered to a wide range of customers and its role as a gateway to other financial sectors.

The credits

Loan-related products (loans) generally present a lower money laundering/terrorist financing risk. Mortgage loans, in particular, require extensive documentation of income, assets and future cash flows, if only to verify credit worthiness (solvency). In principle, loans to legal entities are more susceptible to money laundering than loans to individuals, as they tend to involve more complex structures and larger volumes of transactions. The banking sector in Romania is characterized by a relatively low share of corporate borrowers in the total loan portfolio, as corporates account for only 42% of all loans, 50% of all loans are granted to households, of which mortgage loans account for 30 percent, and the rest are consumer loans. transactions. The banking sector in Romania is characterized by a relatively low share of corporate borrowers in the total loan portfolio, as businesses represent only 42% of total loans, 50% of total loans are granted to households, of which mortgage loans represent 30 percent, and the rest are consumer loans.



However, one of the challenges of lending is updating customer data due to the refusal of some customers to provide data to the institution after the loan is granted, believing that as long as they pay the installments on time there is no reason to interact with the bank. However, the sectoral regulation of the National Bank of Romania provides guidance for such situations.

Current accounts

As regards product-specific risks, it should be mentioned that in Romania current accounts are the basis of a business relationship and serve as a benchmark for other banking products. They are subject to increased risk as funds in current accounts can be highly fungible and liquid and transactions can be carried out in a very short period of time at any time. Cash

can also be deposited and withdrawn at any time, including via ATMs. There is a wide range of distribution channels, including those that support online banking without direct contact with customers. In online retailing, new payment methods are being seen where the payer and payee can be separated, on several levels. This can make it difficult to identify the actual payee or the person who holds the payment account, as instant payment allows amounts to be transferred in real time. Current accounts can also be used for terrorist financing purposes, particularly for small value transactions, as small amounts are harder to identify and trace than larger transactions. According to centralized data from the banking system, the total number of current accounts held by individuals at the end of 2020 was 24,681,152 (regardless of the number of accounts held by each customer and their currency), while the number of customers, individuals, in banks' portfolios was 19,580,567.

Only one bank in the system does not offer current account services to customers, 3 credit institutions do not manage business relationships with individuals, and another bank does not accept business relationships with non-resident individuals.

The number of resident individual customers in the banks' customer portfolios is 19,374,172, representing 98.95% of the total number of customers.

The number of non-resident individual customers in banks' customer portfolios is 206,395, representing 1.05% of the total number of customers.

In terms of distribution channels, 15 banks offer the possibility to initiate business relationships and access products/services remotely, without the physical presence of the customer. Customers with current accounts only in foreign currency represent a certain risk, but the likelihood of it occurring is low, as most banks initiate business relations with a customer by opening an initial current account in RON, because there are a small number of non-resident customers in the banks' portfolios, but also because banks apply additional know-your-customer measures in such circumstances.

Additionally, according to centralized data from the banking system, the total number of business relationships managed by banks with legal entities, for the reference period, is 1,383,138. Four (4) credit institutions do not manage business relationships with legal entities. The number of clients, resident legal entities (with resident real beneficiaries), from the banks' portfolios is 1,271,741, representing 91.95% of the total number of legal entity clients.

The number of clients, resident legal entities (with at least one non-resident real beneficiary), from the banks' portfolios was 107,658, representing 7.78% of the total number of legal entity clients.

The number of clients, non-resident legal entities, from the banks' portfolios was 3,739, representing 0.27% of the total number of legal entity clients.

Although the number of non-resident clients is small, according to the data, the average turnover of non-resident clients is higher than the average turnover of resident clients in the portfolio, an aspect identified in the case of about 60% of banks, which denotes an intense activity of non-resident customers.

Of the total number of clients classified as Publicly Exposed Persons (PEPs) in banks, 95.94% are resident PEPs, while of the total number of non-resident PEPs, 6.57% are PEPs

from high-risk third jurisdictions as determined by European Commission, 52.8% are PEPs from other high-risk jurisdictions, and 37.71% are PEPs from the EU/EEA.

Banking correspondent relationship

Regarding LORO accounts, opened as part of the banking correspondent services offered by credit institutions in Romania, the following aspects must be taken into account:

- Of the 35 credit institutions registered in Romania and branches of foreign credit institutions, 21 offered LORO accounts as bank correspondent services in 2021;
- None of these 21 banks offered "payable-through account" services and only 3 of them, which are part of international groups, established "nested accounts" relationships;
- In 2021, most of the responding credit institutions were registered in the European Economic Area (including Romania). Although more than 50% of the transactional volumes (in terms of amounts) were related to respondent credit institutions outside the European Economic Area, the largest transactional volumes related to this type of correspondent relationship were recorded with institutions in the UK and the USA;
- Credit institutions have policies for accepting correspondent banks in their portfolio and usually establish a list of unacceptable types of correspondent banks (ghost banks, banks offering anonymous accounts, unregulated banks, downstream correspondent banks, etc.) and of unacceptable customers/transactions of the respondent banks (in correlation with their risk appetite, for example: customers in the gaming industry, using virtual currency, customers/transactions related to the production and sale of weapons, customers/transactions related to pornography/ prostitution etc.)

During 2018-2021 there were no closed correspondent relationships due to repeated provision of funds transfers with incomplete/missing mandatory data. The analysis of the banking sector revealed the following risks:

A. *General risks:*

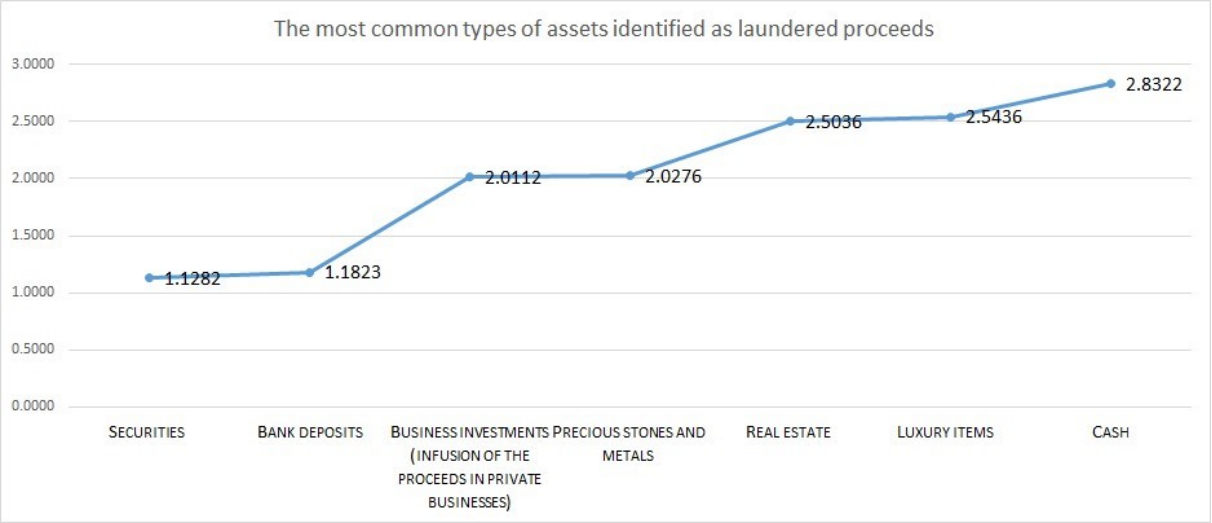
- the evolution of the criminal phenomenon at the national level, the diversification of the operating methods and techniques used by criminals to introduce the proceeds of crime into the banking and financial system;
- the national economic context;
- the political environment;
- the risks generated by the pandemic (trafficking of counterfeit medicines, falsification of medical materials and the sale of consumables without the quality standards required by the health sector; the increase in fraud and financial scams due to economic uncertainty; cybercrime; offering fraudulent investments in the form of Ponzi schemes due to economic uncertainty and derivative methods in the context of the pandemic; the use of virtual assets, as a method of laundering them; possible delays in obtaining additional information necessary for the ongoing analysis or investigation, but also delays in the transmission of STRs; the use abuse of non-profit organizations; temporary or intermittent closure of economic activities that prevent the proper fulfillment of obligations to prevent money laundering and terrorist financing),
- the international climate (the war in Ukraine, terrorist attacks in European cities, the situation in Syria, Iran, North Korea, Russia, the pronounced phenomenon of migration from the Middle East to European states, the situation in Afghanistan),

B. *Technological developments:*
   - Technological progress, the digital revolution, the promotion of new distribution mechanisms and the use of new technologies.

C. *Customer and product categories:*
   - persons/entities that issue/distribute and/or trade in any form electronic/virtual currency;
   - fund transfer operations - because they can constitute a channel for the transfer of funds for the purpose of financing terrorism;
   - developers, real estate promotion and real estate transactions;
   - precious metals/stones (including diamonds) businesses, online casinos/gambling, charities, maritime industry;
   - not updating CAEN codes (Classification of National Economic Activities) to current realities - activities such as currency exchange offices / pawnshops are not differentiated from other financial activities that may present a lower risk related to ML;
   - international fund transfers;
   - speculative transactions for the sale and purchase of agricultural land. The appearance in the field of agriculture in Romania of legal entities owned/controlled by investment funds;
   - establishing business relationships with natural or legal persons associated with non-cooperative countries/countries that do not properly apply FATF standards;
   - initiating / continuing business relations with persons associated with negative events from the point of view of financial crimes;
   - from the perspective of correspondent banking relationships;
   - the transition to a digital activity generated the launch of new specific products/services that allow customers remote access, without the need for their physical presence at the bank.

D. *Banking correspondent relationships:*
   - the lack of standardization of SWIFT/SEPA payment messages, in order to ensure compliance with Regulation (EU) 2015/847, FATF Recommendation no. 16, EBA Guidelines and Guidelines, to ensure the necessary framework for preventing and combating money laundering and terrorist financing, in accordance with legal provisions, in the context where messages accompanying cross-border payments do not contain a separate ISO code field for both the country of the payer/payee bank (customer counterparty) and a separate dedicated field for the country of registration/residence of the payer/ the beneficiary (counterpart of the client).

Additionally, in terms of the most common types of assets that can be introduced into the financial circuit through money laundering mechanisms, according to consultation with compliance officers from credit institutions, on a scale where "rarely = 1", "average = 2", "often = 3".
Thus, securities (guarantees) were considered to be rarely used (1.1282/3), and cash was identified as the most frequently (2.8322/3) used asset for money laundering. At the same time, the other indicators were classified, within the consultation, as being used, as follows: rare: bank deposits (1.1823/3), medium: business investments (infusion of income into private businesses) - 2, 0112/3 and precious stones and metals (2.0276/3) and often used for money laundering: real estate (2.5036/3) and luxury goods (2.5436/3).



Value boxes

A small number of banks consider that there is a "potential" risk of abuse for certain categories of safes. However, there is no evidence of actual abuses and therefore a real danger, since, in accordance with the legislation in the field, know-your-customer measures are also mandatory for this service, and the customers and beneficial owners are registered and reported to the centralized register of bank accounts.

However, the safe can only store goods/money, but is not a way to allow them to enter the financial system. In addition, several banks have introduced into the contract the prohibition to deposit cash in these safes and the condition that, in order to obtain this product, the person is already a client of the bank using other products/services. Most studies and reports have concluded that extending the term "financial intermediation" to purely physical storage of assets would be complex and expected to be associated with high costs. Additionally, it is important to note that the existing regulation in the field is in accordance with international standards.

Given that the need for additional regulation has not been identified, the existing legal framework and the measures implemented by the banks being sufficient with regard to the principle of proportionality, the NBR will nevertheless monitor developments and, if necessary, revise the applicable measures.

Illustrated risks from surveillance activity

As presented in the general part, the NBR assessed the risks of money laundering and terrorist financing, classified banks and established a detailed methodology for a risk-based approach to its supervisory activities in the field of preventing and combating money laundering and terrorist financing.

Conclusion: The banking sector is considered to present an average (residual) risk, partly due to a more mature control environment compared to the rest of the regulated entities. The high average rating set by the NBR for certain institutions, as well as the weighted average rating of the banking sector (3.1) are used for supervisory purposes, resource allocation and also for awareness purposes. The elements taken into account in the determination of the supervisory rating used in the supervisory work are those verified in

accordance with the legal supervisory tasks, focusing on operational risks, governance, deficiencies, but in a broader perspective. Therefore, given the small size of the Romanian financial system in the EU financial market, the lack of complex products (e.g., as presented, private banking) and the limited outreach (very low number of branches abroad), the money laundering/terrorist financing risk associated with this sector, from the perspective of the national risk assessment, is considered medium (based on the ratings in the Council Assessment Methodology). Another element is the very demanding regulation of know-your-customer measures, the number of documents required, the sources of information and supporting documents, as well as continuous updating and verification are very strict for the financial sector supervised by the NBR. It should be noted that this applies to the entire sector supervised by the NBR.

In general, the legislation is implemented effectively using the risk-based approach. Due to the detailed requirements, banks focus very much on initial customer identification. Identification in bank branches - face-to-face identification - continues to be the most commonly used method of identification. Careful initial identification should be followed by regular and ongoing identity verification, with comprehensive monitoring of the business relationship and transactions. As financial intermediaries, banks are extremely important to the economy because of their business support functions and international interconnectedness. High turnover volumes and the sector's natural focus on asset management and transfer may mean that the banking sector as a whole is naturally exposed to a higher risk of money laundering. The risk of the banking sector as a whole being misused for money laundering is assessed as medium. However, mitigating factors keep the overall risk of the sector at medium level, as the quality and effectiveness of general controls in the area of prevention and combating money laundering and terrorist financing are considered adequate, with insufficient resources being the main problem. In recent years, the quality and effectiveness of supervisory procedures and practices have been continuously improved.

2. Sub-sector of non-banking financial institutions (NBFIs) (loan/leasing companies)

Non-bank financial institutions (loan/leasing companies) - (NBFIs) are companies authorized to carry out lending activities and, where appropriate, payment services and other ancillary activities. Loan/leasing NBFIs are not allowed to receive deposits or other repayable funds. Loan/leasing NBFIs are registered by the NBR, depending on the type and volume of their lending activity, in order to carry out their lending activity. Loan/leasing NBFIs registered in the General Register which exceed a threshold set by the NBR such that their activity is of enhanced interest from a financial stability perspective, are also registered in the Special Register if the cumulative level of own capital and sources borrowed on the basis of outstanding loan/financing contracts is at least RON 50,000,000, the cumulative level of loans/financing granted and commitments entered into is at least RON 25,000,000 and the total volume of consumer loans granted in the last three quarters exceeds RON 75,000,000.

As mentioned, in order to prevent money laundering and terrorist financing, the NBR is responsible for the regulation and supervision of only loan/leasing NBFIs registered in the Special Register, and those registered only in the General Register or in the Special Register are supervised by NOPCML.

Loan/leasing NBFIs registered in the Special Register can carry out the following lending activities:

a. granting loans, including but not limited to: consumer loans, mortgage loans, real estate loans, microloans, financing of commercial transactions, factoring operations, discounting, lump sums;
b. financial leasing;
c. issuing guarantees, assuming guarantee commitments, assuming financing commitments.

In the 2019-2021 period, the number of institutions regulated and supervised by the NBR increased slightly, as well as the balance of loans granted by these institutions:

	31.12.2019	**31.12.2020**	**31.12.2021**
Number of institutions regulated and supervised by NBR	69	69	73
The balance of loans granted by the institutions regulated and supervised by NBR	7,123,153,913 Eur	7,148,774,694 Eur	7,637,064,934 Eur

The sub-sector represented by Loan/Leasing NBFIs is low-risk, as the client portfolio is almost entirely composed of residents, as noted in the chart below, and the only products are lending products.

Total no of customers	Residents	Non-resident and	Individuals	Companies	Low risk	Medium risk	High risk
1,953,822	1,953,747	75	1,661,870	291,950	71.63%	25.52%	2.85%

In terms of products, services and risk factors of transactions in this sub-sector, according to the latest EBA[22] Risk Factor Guide, they are more associated with low risks, such as a low-value loan facility, including one that is conditional on the purchase of a particular consumer good or service, a low-value product, a leasing contract, where the legal and beneficial title to the asset is not transferred to the customer until the contractual relationship is terminated, the transactions are largely carried out through an account opened in the customer's name with a financial institution subject to AML/CTF requirements.

Also, almost none of the higher risk factors related to products are specific to this sub-sector, except for new products associated with online registration mechanisms, which are starting to be promoted, especially since the outbreak of the pandemic, and which pose some risks related to identity theft. To reduce this risk, the Romanian Digitization Authority has adopted specific requirements. At the same time, the NBR has supported a new legislative initiative/draft law that will allow supervised entities to access the Ministry of Internal

22

https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/Guidelines%20on%20ML-TF%20risk%20factors%20%28revised%29%20202102/Translations/1016927/Guidelines%20ML%20TF%20Risk%20Factors_RO.pdf

Affairs' database with information on people's identity documents. In the meantime, the NBR is sending letters to all supervised entities with warnings about any suspicion of identity theft/forged identity documents and issuing guidance on developments in the associated distribution channels.

In many respects, the very nature of leasing makes the industry low risk from a money laundering perspective, and this is the general view. For example, in a leasing contract, no funds are transferred to the lessee (the user), but instead the customer is granted the right to use an asset (e.g. equipment or a vehicle). In this way, the way leasing contracts are set up clearly does not lend itself to being used for money laundering or terrorist financing, as the funds are almost always paid directly into the supplier's bank account. In addition to the nature of the relationship between the lessor, lessee and supplier, the duration of the leases as well as the payment methods used by lessees to make repayments contribute, also reduce the risk of money laundering in leasing. Leases are generally long-term, with an average duration of between 3 and 5 years. In addition, in the vast majority of cases, repayments to lessors are made by direct debit or payment order from the lessee's bank account, which means that the necessary checks consisting of know-your-customer measures will have been carried out by the customer's financial institution before being subject to further checks by the leasing company.

Also, another fact to consider is that the compliance systems and resources of these non-bank financial lending institutions are not comparable to those of banks. Only those that are part of a group that benefits from the support of the parent bank have access to such resources. The same legal requirements and supervisory objectives were and are applicable to all supervised institutions.

The main vulnerabilities identified in the supervision process at the level of (some) non-bank financial lending institutions are:

- Inadequate risk assessment methodology and risk assessment or assessment process used in relation to distribution channels;
- lack of procedures or inadequate procedures and control systems regarding the implementation and efficiency of know-your-customer measures;
- the high turnover of staff performing KYC/AML/CTF activities, including at the level of the compliance officer responsible for coordinating the implementation of legal provisions;
- lack of a training program for employees carrying out KYC/AML/CTF activities (for example: not including aspects related to types of suspicious behavior, the legal and internal framework of KYC/AML or the absence of final assessment tests taken by employees at the end of the training program).

However, the overall risk of the sub-sector is low due to the limited nature of the products, the limited possibility of geographical coverage, the fact that most of the supervised entities have resident persons in the customer portfolio and offer leasing and small loans. Due to the specific nature of the business, in order to reduce credit risk, institutions collect all relevant information about customers, their source of funding, etc., and it occurs in the case of loans with significant collateral, early repayments that do not match the customer's financial situation or from third parties unrelated to the customer, but such situations were very few.

In addition, in accordance with the ESA Joint Guidelines on cooperation and exchange of information for the purposes of Directive (EU) No 2015/849 between competent authorities supervising credit institutions and financial institutions, representatives of the NBR

participate in the AML/CTF supervisory boards (AML/CTF) of the competent authorities supervising loan/leasing NBFIs.

It should be noted that, at the time of establishment, these loan/leasing NBFIs are under the supervision of the NOPCML and, once they reach a certain level of importance in their activity, they come under the supervision of the NBR. At the time, there is close communication between them and the NBR to ensure that the former are aware of their (new/additional) anti-money laundering and anti-terrorist financing obligations under sectoral legislation. They must demonstrate that they have the appropriate strategy, risk assessment and procedures in place. As of 2021, meetings are held individually for each institution with the persons responsible for the implementation of legislation in the field of prevention and combating money laundering and terrorist financing and international sanctions and information is requested on their work, client portfolio, human resources involved in the activities to prevent money laundering and terrorist financing, etc. Similarly, such meetings are held with loan/leasing NBFIs classified as high risk compared to other entities in their sub-sector to discuss measures to be implemented to reduce the level of risk/timeline of activities in the supervisory program, etc.

Taking into account the above elements as well as the results of the inspections (supervisory actions) carried out, the loan/leasing NBFIs have been grouped into 4 groups.

The level of supervisory engagement will be determined in proportion to the degree of ML/TF risk associated with each NBFI according to the most recent available assessment, and according to the group into which it falls.

It should be noted that the same requirements for know-your-customer measures as for banks are applicable to loan/leasing NBFIs. In addition, for any type of loan/leasing, NBR Regulation No 17/2012, as amended, sets out a number of obligations for supervised entities regarding the types of income considered eligible by the lender, in particular that lenders must analyze income for the previous year based on documents proving the income declared to the tax authorities and/or documents proving the income received on accounts opened with the loan institution. In cases where there is no legal obligation to declare income to the tax authorities, creditors shall establish the income for the previous year on the basis of other supporting documents that demonstrate its continuity. Supporting documents are also needed to prove changes in the client's income declaration, such as a change of job, or changes that have a significant impact on the growth of the self-employed person's business. Such measures provide a better picture of the source of funds and traceability, which would allow the detection of money laundering through loan/leasing and early repayment of criminal proceeds. Any shortcomings in the implementation of these requirements will be brought to the attention of the Money Laundering and Terrorist Financing Prevention Service by prudential supervision to examine the implications from this perspective.

In terms of structure, consumer credit and credit cards account for 99% of all loans granted by loan/leasing NBFIs. As regards the corporate sector, only 6% of the amounts outstanding are credit lines, with loans to finance assets and equipment accounting for about 32% of total exposures of loan/leasing NBFIs. Against the backdrop of the epidemiological situation in Romania, Loan/Leasing NBFIs were less active in the credit market in the months immediately following the pandemic, a situation driven both by lower demand (in the context of high uncertainty about the future financial situation of both companies and a population) and lower supply (as a result of increased risk aversion towards companies from sectors affected by restrictions or towards individuals operating in sectors affected by downsizing).

In the context of the launch of two government programs ("SME Leasing" and "SME Factor"), loan/leasing NBFIs are eligible for funding and may recover in the near future. These economic developments also reflect on risk appetite and reduce pressure on financial crime departments.

No.	Elements	Likelihood Rating (L)	Assessment of consequence (C)	Risk rating
	Risk associated with the Subsector of non-banking financial institutions (NBFI) (loan/leasing companies)	**low**	**low**	**low**
Associated vulnerabilities: **Limited control of the customer relationship - once credit has been granted, there are no tools to change the course of the business relationship.**				
Event description: **Using the loan as justification for illegal money, by repaying in advance from unknown/unclear sources**				
Risk description: **The probability is very low** **Consequences are low,** **The risk is low**				

3. Electronic Money Issuing Institutions (EMII) sub-sector

Currently, there are 5 institutions issuing electronic money supervised by the NBR in the field of preventing money laundering and terrorist financing:

- 2 institutions issuing electronic money, Romanian legal entities (one of which is also a non-bank financial institution registered in the Special Register)
- 3 branches of electronic money issuing institutions from other member states

The money laundering and terrorist financing risk associated with electronic currency, which typically offers a fast and often anonymous payment option, has been documented by FATF and Moneyval. In Romania, for a better management of these risks, the legal framework does not exempt any type of electronic currency from the application of due diligence measures, and therefore no anonymous electronic currency can be issued by entities authorized by the NBR.

In terms of sector size, as of 30/06/2020, all EMIIs, including branches, had 225,905 customers, of which only 34 were non-residents.

Total number of customers	residents	non residents	Individuals	Trade companies	Low risk	Medium risk	High risk
225,905	225.871	34	224,442	1,463	57.14%	39.39%	3.47%

The sector is mainly involved in providing payment services to its customers and therefore also offers cross-border payment services. In the period between 01.07.2019 and 30.06.2020, the total value of cross-border payments received was of EUR 9,039,168 (65% from the UK,

Austria and Germany) and the value of cross-border payments ordered was of EUR 3,187,997 (74% to China, Turkey and Belgium).

As regards the risks related to the issuance of e-money by EMIIs, it is noted that they provide e-wallets to their customers and the offer does not include anonymous cards. Although the product allows peer-to-peer transfers exclusively between EMII customers, there are limits on the value of transactions. The e-money product can be funded by card or bank transfer from a RON account with a credit or financial institution in the EEA. Cash deposits and withdrawals at ATMs can only be done by the customer, with low limits per transaction and per day: the limit for daily cash deposits or withdrawals is capped at RON 10,000/day, with additional limits: a limit of RON 500/1,000 per location, and deposit or withdrawal can only be done by the customer (no third parties can be involved in the transaction).

Thus, a customer wishing to use the maximum daily limit would have to visit 10-20 dealer locations and deposit/withdraw the maximum amount at each location. Cash withdrawals using linked debit cards have daily and monthly limits based on the amount and number of transactions. The institution has set up an automated scenario-based transaction monitoring system with several scenarios designed to identify all cases where customer transactions exceed normally expected withdrawals (upon registration, customer makes cash transactions close to the maximum allowed amount; multiple cash receipts/deposits in a given period (day/week/month); multiple cash receipts followed by a peer-to-peer/cash withdrawal, etc.). According to the results of the on-site inspections, the risk rating of the EMII sub-sector was assessed as medium-risk (3).

No.	Elements	Likelihood Rating (L)	Assessment of consequences (C)	Risk Rating
	Risk associated with the sub-sector Electronic Money Issuing Institutions (EMII)	**low**	**severe**	**medium-high**
Associated vulnerabilities: **Low quality controls and poor reporting.**				
Associated threat: **Applicable customer awareness measures and ongoing monitoring may not detect problems in time.**				
Event description: **Criminals can exploit the vulnerabilities**				
Risk description: medium-high ***Probability is low, Consequences can be severe.***				

4. Payment institutions sub-sector (PI)

Globally, money remittance firms (including payment and e-money institutions) are commonly used by criminals involved in money laundering or terrorist financing, given the international payments, speed and volume of transactions and the geographical coverage.

There are currently 13 payment institutions supervised by the NBR in the field of money laundering and terrorist financing prevention:

- 9 payment institutions, Romanian legal entities (4 of which are also non-bank financial institutions registered in the Special Register)
- 4 branches of payment institutions from other Member States

As regards the size of the sector, it should be taken into account that, as of 30.06.2020, 45.56% of PIs' customers were customers of payment institutions that also had the status of non-bank financial institutions, whose main activity is lending.

NBR authorized PIs to operate mainly in Romania, without branches or subsidiaries abroad, and only 2 entities have transferred their activity to other Member States (an EMII and a PI, both Romanian legal entities), but at the end of 2020 none of them were actively providing services in other Member States. Also, with 2 exceptions: one payment institution has an agent (credit institution) in the Republic of Moldova, one e-M institution has an agent in Switzerland (inactive, according to the information obtained during the on-site surveillance action in November 2020), and all their agents are Romanian entities.

In terms of global coverage, in the period between 01.07.2019-30.06.2020, the total value of cross-border payments received was EUR 159,962,145 (UK, Spain, Italy, Germany and Ireland accounting for 78.50% of total receipts) and the value of cross-border payments made was EUR 286,205,254 (75.59% of total payments made went to the UK, China, Germany, Poland, Hong Kong and Bulgaria).

According to the results of the on-site inspections, the risk rating of the payment institutions sub-sector was assessed as medium-critical (3). It should be noted that 3 of the 13 institutions have not previously been subject to supervisory actions in the area of prevention of money laundering and terrorist financing completed with a risk profile assessment, as one institution was licensed in April 2021 and 2 institutions were passporting in September 2021. The level of risk is mainly a consequence of deficiencies identified in the assessment of customer-related money laundering and terrorist financing risk, the application of standard and additional know-your-customer measures, ongoing monitoring policies and procedures and the effectiveness of suspicious transaction reporting (STR), the quality of controls, staff training, as well as misalignment of internal regulations with some requirements set out in primary legislation. Also, as a result of the COVID-19 pandemic, there has been an increase in the number of entities offering online enrolment services, with many entities using this way of initiating business relationships for the first time, in many cases without the means of electronic identification or relevant trust services as required by Regulation (EU) No 910/2014 of the European Parliament and of the Council, which exposes the sector to additional money laundering and terrorist financing risks.

In some cases, the risks associated with identity theft have already manifested themselves. Checking how entities assess the ML/TF risks associated with digitization projects and the adoption of FinTech solutions/new technologies is one of the strategic priorities of the on-site inspections carried out by the NBR.

No.	Elements	Likelihood Rating (L)	Assessment of consequences (C)	Risk Rating
	risk associated with	**Low**	**high**	**medium-high**

	the subsector of payment institutions (PI)			
Associated vulnerabilities: **Lack of knowledge of the customer's transactional behavior**				
Associated threat:				

Deficiencies in risk understanding
Event description: **Should anyone ever intend to use the system for terrorist financing activities**
Risk description: medium-high **The probability is low,** **The consequences can be severe if they are used to finance terrorism.**

5. Agents of foreign PIs and EMIIs

Agents and distributors are not reporting entities under the law, so their obligations are contractual, with the mandating payment institutions/electronic money issuers. Therefore, the ultimate responsibility for ensuring compliance with legal requirements for activities carried out by mandated third parties, including in relation to the prevention of money laundering and terrorist financing, remains with the mandating PIs/EMIIs and, by implication, the supervisory authorities in their home jurisdictions. National payment institutions offering remittance services cover a limited number of transaction corridors, so large international PIs are the main options for international transactions, including those to high-risk jurisdictions. In 2020, the value of remittances from abroad was €2,171,086,944, with remittances abroad accounting for less than 11% of this amount, i.e. €237,148,005.

These entities operate in Romania through an increasing number of agents: from 845 agents on 31.12.2018, to 1,748 agents on 31.12.2019, to 2,542 agents on 30.06.2020. The most important increase is registered among agents who are "retail stores" (whose number reached 2,211 agents as of 30.06.2020, respectively 87% of the total agents), entities with a limited understanding of the risks of money laundering and terrorist financing. In this context, we note that, compared to their number, the volume of their transactions is limited: approx. 7% of the total volume of lending transactions and approx. 3.5% of the total volume of debit transactions.

Most transactions through money remittance services are processed through entities supervised by the NBR (banks, PIs), which represent approximately 39% of the volume of credit transactions and approximately 57% of the volume of debit transactions. Foreign exchange offices account for approximately 30% of the volume of credit transactions and approximately 18% of the volume of debit transactions.

Regarding the geographical distribution, more specifically, third countries with high risk and strategic deficiencies[23] (HRTC), the total volume of transactions involving these jurisdictions represents 0.58% of the total volume of cross-border transactions carried out by money remittance service providers in 2020 (0.36% in the case of credit transactions and 2.74% in the case of debit transactions). For this estimate, we have also included HRTCs that were on the FATF list in 2021, although at the time of the financial flows in 2020, these countries were not on the FATF list of monitored jurisdictions, so the estimated volume is much lower.

[23]Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies, as amended: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R1675-20210207
- *FATF list of High-Risk Jurisdictions subject to a Call for Action*: http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-february-2020.html
- *Jurisdictions under Increased Monitoring* – February 21, 2020: http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-february-2020.html
- *FATF Jurisdictions under Increased Monitoring* – June 2021: http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-june-2021.html

Despite the lack of full supervisory powers, a specific concern is related to the activities carried out by entities from other member states that operate in Romania through agents and distributors, certain risks being identified.

Risks arising from the size and structure of agent networks:

As previously mentioned, payment institutions (PIs) and electronic money issuing institutions (EMIIs) authorized in a member state can provide payment services and distribute electronic money on the territory of other member states through third parties, respectively - natural or legal persons - agents and distributors. Agents and distributors are not reporting entities, respectively they are not part of the categories of entities that are the explicit object of the set of legal obligations to prevent and combat money laundering.

According to the data collected through the 2020 AML/CTF questionnaire, less than 10% of the PIs offering money remittance services are also reporting entities (banks, payment institutions, exchange offices, gambling service providers), which means that a significant number of agents have a limited understanding of money laundering/terrorist financing risks, relying solely on the (limited) training provided by PIs. In addition, the size of the agent network of an entity providing money remittance services can pose a challenge for the trustee in maintaining adequate oversight of its agents to ensure that they comply with legal and regulatory requirements.

In accordance with the EBA Guide on the cooperation and exchange of information for the purpose of Directive (EU) 2015/849 between the competent authorities that supervise credit and financial institutions, the representatives of the National Bank of Romania participate in the AML/CFT colleges (AML/CTF) of the competent authorities which oversees PIs and EMIIs. Thus, in this framework of cooperation, the representatives of the supervisory authorities present the results of the inspection actions, with incidence on serious violations of the legislation and rules for the prevention of money laundering and the financing of terrorism.

The supranational assessment of money laundering and terrorist financing risks in the internal market and in relation to cross-border activities, which was published by the European Commission on 24.07.2019, identifies, in particular for money remittance services, carried out through money remittance service providers with an extensive network of global agents, a significant level of money laundering and terrorist financing risk (level 4/4). The high level of risk is due to the fact that money remittance services are frequently used for money laundering and terrorist financing and are easily accessible without specific knowledge or prior planning. Remittance service providers mostly rely on agents to carry out their business and therefore agents are their main risk factor.

In the case of EMIIs, their services may be attractive to criminal organizations, in particular with regard to the use of prepaid cards and vouchers that can be purchased in cash and used online or offline, with certain exceptions to the application of know-your-customer measures.

In the case of agents/distributors, the risk of the sub-sector is considered medium-risk (level 3), due to the elements presented above and given the large amounts of money used at sub-sector level and the high degree of anonymity of transactions.

4.2.3 Expected developments

The level of proceeds from traditional crime could fall in favor of cybercrime, such as internet fraud, hacking and identity theft, which are on the rise. Also, Europol's IOCTA Report 2021 shows[24] how cybercrime continues to grow.

In the area of cybercrime, a shift towards bigger and more profitable targets and new technologies can be observed. According to Europol, new threats arise not only from the use of new technologies, but also by exploiting long-known vulnerabilities in existing technologies.

Further amendments to Law 129/2019 on suspicious transaction reporting may raise new challenges for the financial system to adapt IT systems and establish valid and effective scenarios. The repeal of the provisions in the primary legislation on the submission of a suspicious transaction report with regard to elements that are likely to raise suspicions about the nature (character), economic purpose or motivation of the transaction, such as the existence of anomalies in relation to the customer profile, as well as when there are indications that the data held about the customer or the beneficial owner are not real or up-to-date, and the customer refuses to update them or provides explanations that are not plausible, leads to the removal of the link between customer monitoring activity and STR reporting. The current provisions in force, which stipulate the obligation to report only if the assets originate from the commission of crimes or are related to terrorist financing, or if the information the reporting entity holds can be used to enforce the provisions of this law, do not provide real tools for calibrating the systems. This will most likely trigger a reduction in the number of STRs sent by the financial system.

Conclusions:

The banking sector has a medium residual risk, mainly due to the more complex and mature control environment compared to the rest of the regulated entities.

The overall risk of the **lending/leasing non-bank financial institutions** sub-sector is low, due to the limited nature of the products, low geographical coverage and the fact that most entities have resident customers in their portfolio and offer leasing and small value loans.

The sub-sector of e-M institutions is medium to medium risk. The level of risk is due to identified weaknesses.

The payment institutions sub-sector has been assessed as medium to medium risk, mainly due to identified weaknesses.

The sub-sector of electronic money dispensers/payment agents is assessed as medium to medium risk.

4.3. Non-banking financial sector (financial instruments, insurance and private pension fund managers)

---

24 https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

4.3.1. General description of the sector

The Financial Supervisory Authority (hereinafter referred to as the FSA) is the non-banking financial supervisory authority for the financial instruments sector, the insurance and reinsurance sector and the private pension sector. The FSA is an autonomous, specialized administrative authority with legal personality, independent, self-financed, established by Government Emergency Ordinance No 93/2012, as amended, with the role of regulating, authorizing, supervising and controlling the supervised entities.

In addition, the FSA has exclusive regulatory, supervisory and inspection (control) powers with regard to compliance with the provisions of Law no. 129/2019 (Law on preventing and combating money laundering and terrorist financing) and the secondary regulations issued in application thereof by the non-banking financial institutions (hereinafter referred to as NBFIs) under its supervision, in accordance with the powers set out in the specific legislation. This also includes foreign branches of NBFIs operating and having a physical presence in the jurisdiction of Romania[25]. The FSA may order NBFIs that do not comply with the provisions of Law no. 129/2019, secondary regulations or other measures ordered under the aforementioned law, measures to remedy deficiencies and/or sanctions in order to mitigate risks or remedy deficiencies and their causes.

The FSA has independence in the considerations of timeliness of the qualitative assessments and analyses underlying the issuance of its acts.

With regard to the category of entities supervised by the FSA from the perspective of the legal framework for preventing and combating money laundering and terrorist financing, these are those referred to in Article 5 paragraph (1) letter (b) and Article 2 letter (g) paragraphs (2) to (7) of Law 129/2019, which do not overlap entirely with those supervised under sectoral (prudential) legislation, namely:

- insurers, composite insurers, captive insurers, micro insurers, as defined in Article 1 paragraph (2) of Law No 237/2015 on the authorization and supervision of insurance and reinsurance activity, as amended and supplemented, when carrying out insurance activities, including distribution activities, in connection with investment-based insurance products, as defined in Article 3 paragraph (1) point 23 of Law No 236/2018 on insurance distribution, as amended; with life insurance products, as defined in Annex No. 1 Section C "Life insurance" of the Law No. 237/2015, as amended, or with those included in the guarantee insurance category, as defined in Annex No. 1 Section A point 15 of the Law No. 237/2015, as amended, insurance intermediaries, as defined in Article 3 paragraph (1) point 11 of the Law No. 236/2018, as amended, when distributing investment-based insurance products, as defined in Article 3 paragraph (1) point 23 of Law no. 236/2018, with subsequent additions;
- reinsurers, including captive reinsurers, as defined in Article 1(1) of Regulation (EC) No 236/2010 (2) of Law no. 237/2015, as amended, and reinsurance intermediaries, as defined in Article 3 paragraph (1) point 13 of Law no. 236/2018, as amended;
- central depositaries, alternative investment fund managers, central counterparties, financial investment services companies and other entities authorized under national law to provide investment services and activities, investment management companies, investment firms, entities managing a trading venue;

[25] Article 28 paragraph (1) of Law no. no. 129/2019

- managers of voluntary and/or occupational pension funds, on their own behalf and for the voluntary pension funds and/or occupational pension funds they manage;
- branches situated in a Member State of the financial institutions referred to above, whether their head offices are situated in a Member State or in a third country;

Depending on the type of entity, on December 1st, 2020, the FSA supervised the following entities:

- Capital market/financial instruments: 19 intermediaries (including 1 in withdrawal process, one suspended on request and one suspended due to non-fulfillment of authorization conditions); 9 credit institutions[26], of which 4 also act as depositors in investment fund assets; 18 asset management companies (hereinafter referred to as AMC); 5 autonomous investment companies (hereinafter referred to as "AIC") and the Property Fund; 107 investment funds (81 UCITS and 26 FIA); 9 branches of investment companies from member states (of which 3 were eliminated from 01.01.2021 being from the UK); 4 investment advisers, of which 3 individuals and one legal entity;
  1 central depository (hereinafter referred to as 1 CD); 1 market operator – Bucharest Stock Exchange (hereinafter referred to as "BSE");
- Insurance Market: 28 insurance entities and 11 branches, of which 7 life insurance entities, 3 branches and 284 insurance intermediaries, 19 branches;
- Private Pension System (Optional and Occupational): 8 administrators of optional pension funds[27] (pillar III), 0 administrators of occupational pension funds.

The FSA is the supervisory authority which has the competence to supervise compliance by non-banking financial institutions with the obligations provided for by Law no. 129/2019 (hereinafter referred to as the "Law on the Prevention and Control of Money Laundering and Terrorism Financing"), to inform the criminal investigation bodies and notify the NOPCML (FIU Romania) when, in the exercise of its specific duties, it discovers facts that would could be related to money laundering/terrorist financing[28].

General statistical data on the non-banking financial market

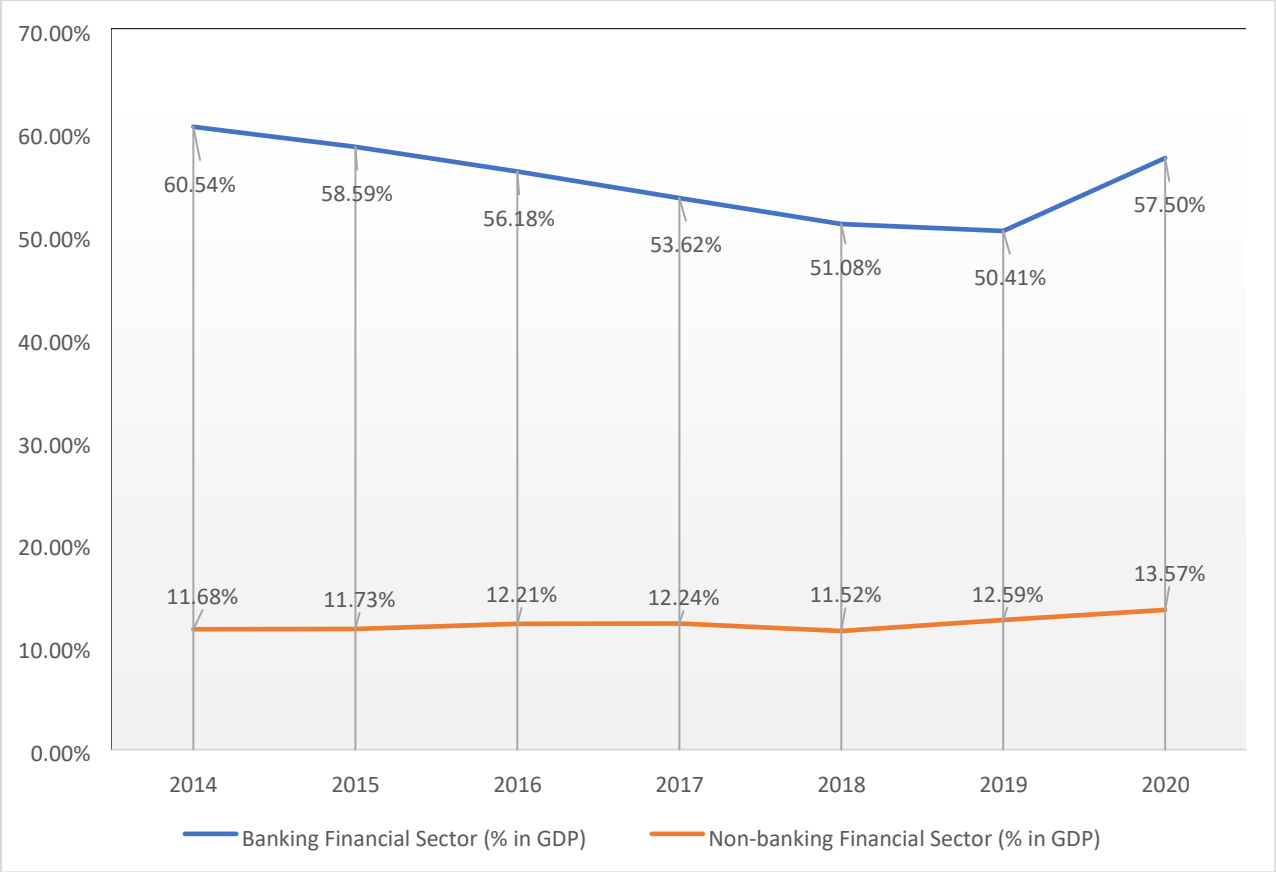
The growth of financial sector assets relative to GDP was sustained from 2014 to 2017, followed by a decline in 2018 and a recovery starting in 2019 compared to 2017. The latest statistical data, for a full year in terms of information financial audited, are reported in 2020, when non-banking financial sectors represented 13.573% of GDP. Thus, the assets of the non-banking financial sector amounted to 143.46 billion lei, with an increase of 8% compared to the end of 2019[29], although in percentage terms the gross domestic product decreased by 3.9% in 2020 compared to 2019.

[26]Total assets in the amount of 84,989.65 million lei on 30/07/2021, at the rate of 4.91/EUR

[27] There are no branches

[28]Article 26 paragraph (2) of Law no. no. 129/2019

[29]According to the data published by the INS

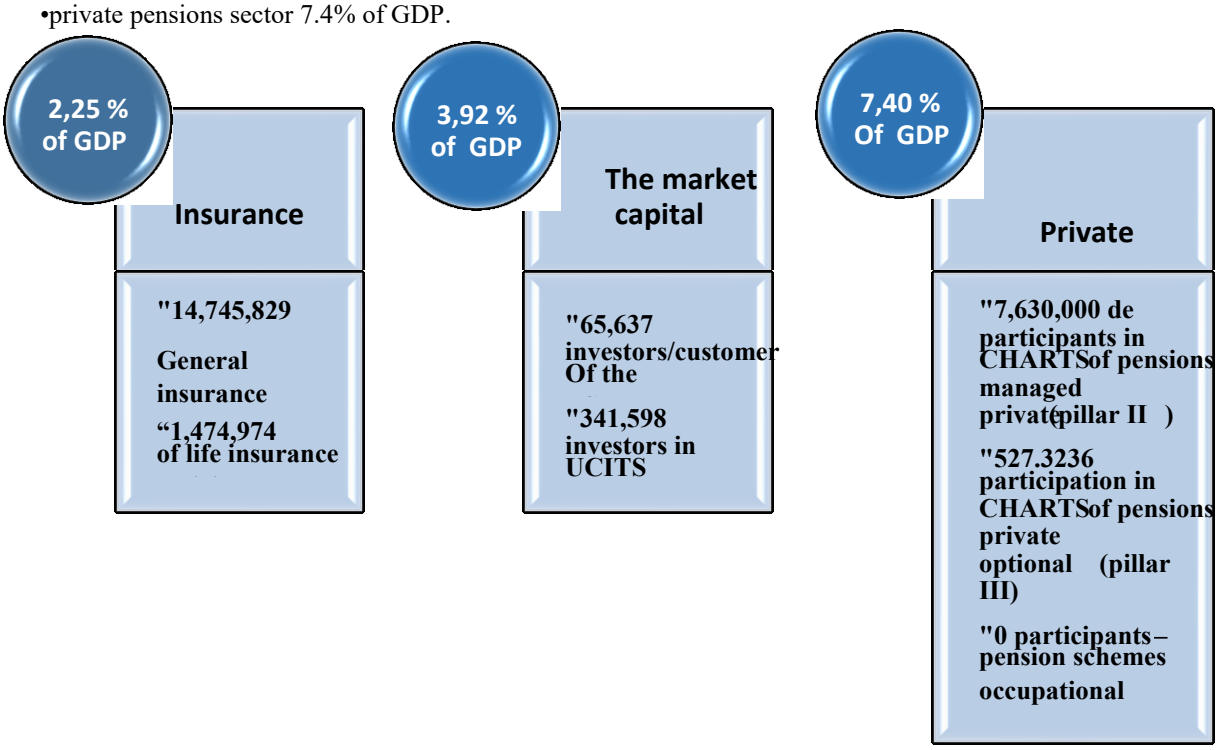


share from gdp[30]	2014	2015	2016	2017	2018	2019	2020
The banking sector (% of GDP)	60.53%	58.59%	56.18%	53.62%	51.09%	50.41%	57.51%
The financial sector non-bank * (% of GDP)	11.69%	11.74%	12.21%	12.24%	11.53%	12.59%	13.57%
Capital market	5.89%	5.80%	5.43%	5.07%	4.15%	4.40%	3.92%
Private pension system	3.01%	3.64%	4.32%	4.84%	5.21%	6.10%	7.40%
sector insurances – reinsurance	2.79%	2.30%	2.47%	2.32%	2.16%	2.10%	2.25%
the relative value of GDP the financial sector	72.22%	70.33%	68.40%	65.86%	62.61%	63.01%	71.08%

The differentiated share in GDP of the non-banking financial sectors on 31.12.2021 is as follows:

[30]Source: INS, NBR, FSA, * NFI calculations are not included

•insurance and reinsurance sector 2.25% of GDP,
•financial instruments sector 3.92% of GDP,
•private pensions sector 7.4% of GDP.



4.3.2. Financial Instruments and Investments Sector (capital market, including voluntary private pension schemes and occupational pension schemes)

As of September 21st, 2020, the Romanian equity market has become an emerging market following the decision of global index provider FTSE Russell. This event was the achievement of the major objective of the STEAM project (Set of Actions for Establishing and Awareness of Emerging Market Status) carried out by the FSA since 2014. In the framework of this strategic project of the Authority, the following measures were taken:

The legal framework on the capital market was revised by:

- Law no. 24/2017 on issuers of financial instruments and market operations;
- Law no. 126/2018 on securities markets,
- Law no. 243/2019 regarding alternative investment funds (hereinafter referred to as AFI) and Law no. 29/2017 regarding open-ended collective investment funds (called open-ended investment funds or OPCVM).

Also, based on a FTSE Russell analysis, equity markets are classified as: Developed, Emerging, Secondary, with regional position, respectively the Bucharest Stock Exchange (referred to as BSE) in terms of volatility, and the correlation between economic growth and index value is similar to (a) advanced emerging market such as Greece, Hungary and the Czech Republic and (b) frontier market such as Bulgaria, Croatia, Slovakia, Slovenia and Cyprus. Romania's market capitalization in GDP was 15.4% in 2020; thus, lagging behind regional markets such as Hungary, Czech Republic and Bulgaria, the market capitalization (including the main segment and MTS) decreased by 15% in 2020 compared to 2019 EUR 32.82 billion (equivalent to RON 164.1 billion) compared to EUR 33.7 billion (equivalent to RON 168.5 billion). Therefore, the total market capitalization is

on the main and alternative equity trading segments, although each stock exchange has a different structure.

The activity recorded by the BSE in 2020 underlines the lack of new IPOs (initial public offers) concluded in the main segment, the most recent having taken place in 2018 (Purcari Wineries) and 2017 (DIGI Communications, SPHERA Franchise Group, AAGES and Transilvania Broker de Asigurare). However, despite the pandemic, 2020 and early 2021 saw increased momentum in the MTF (multilateral trading facility) segment, with nine listings between March 2020 and April 2021: three IT companies (2Performant Network, Safetech Innovations and Firebyte Games), two agricultural companies (Norofert and Holde Agri Invest), two specialist retail companies (Agroland and MAM Bricolaj), one real estate investor (Star Residence Invest) and one industrial manufacturer (Raiko Transilvania). With these new market listings, SMT's market capitalization increased by around 7% in 2020, then by almost 10% in the first quarter of 2021, reaching a market capitalization of EUR 2.2 billion (RON 10.8 billion) at the end of March 2021.

Bucharest Stock Exchange (BSE) was included in the emerging secondary markets category according to the FTSE Russell classification as of 21 September 2020, and Romania's promotion to emerging secondary market status was successful only after Banca Transilvania and Nuclearelectrica met the upgrade criteria for inclusion in the FTSE AllCap index, Bittnet Systems and TeraPlast were also included in the emerging markets micro index.

Capital market institution

Autoritatea de supraveghere financiară (ASF)	Bursa de Valori București (BVB)	Depozitar central (DC)	Fondul de compensare pentru investitori (FCI)
• O autoritate administrativă autonomă, independentă, autofinanțată, care exercită competențe în temeiul prevederilor Ordonanței de urgență a Guvernului nr. 93/2013, aprobată cu modificări prin Legea nr. 113/2013, prin achiziționarea și reorganizarea tuturor competențelor și prerogativelor Comisiei Naționale pentru Valori Mobiliare, Comisiei de Supraveghere a Asigurărilor și Comisiei pentru Supravegherea Sistemului de Pensii Private.	• Un organism de autoreglementare, Bursa de Valori București, adoptă norme și proceduri corespunzătoare, care ulterior sunt supuse aprobării Comisiei Naționale a Valorilor Mobiliare (Autoritatea Supraveghere Financiară).	• Depozitarul central furnizează servicii de compensare, decontare, registru, depozit și custodie pentru valorile mobiliare tranzacționate pe piețe reglementate și sisteme alternative de tranzacționare, precum și orice alte operațiuni conexe.	• Obiectul principal de activitate al Fondului este de a colecta contribuții de la membri și de a plăti compensații investitorilor atunci când un membru nu returnează banii și/sau instrumentele financiare datorate de investitori sau care aparțin acestora, care au fost deținute și/sau gestionate în numele acestora pentru furnizarea de servicii de investiții, până la limita de compensare stabilită în conformitate cu reglementările emise de ASF. Toți intermediarii autorizați să furnizeze servicii de investiții și societățile de administrare a investițiilor care gestionează portofolii individuale de investiții trebuie să fie membri ai fondului.

Autoritatea de Supraveghere Financiara (ASF) - Financial Supervisory Authority (FSA)
O autoritate administrativa, autonoma, independenta, autofinantata, care exercita competente in temeiul prevederilor Ordonantei de urgenta a Guvernului nr. 93/2013, aprobata cu modificari prin Legea nr. 113 / 2013, prin achizitionarea si reorganizarea tuturor competentelor si prerogativelor Comisiei Nationale pentru Valori Mobiliare, Comisiei de Supraveghere a Asigurarilor si Comisiei pentru Supravegherea Sistemului de

Pensii Private. - An autonomous, independent, self-financing administrative authority, exercising competences under the provisions of Government Emergency Ordinance no. 93/2013, approved with amendments by Law no. 113 / 2013, by acquiring and reorganizing all the competences and prerogatives of the National Securities Commission, the Insurance Supervisory Commission and the Commission for the Supervision of the Private Pension System.

Bursa de Valori Bucuresti (BVB) - Bucharest Stock Exchange (BSE)

Un organism de autoreglementare, Bursa de Valori Bucuresti, adopta norme si proceduri corespunzatoare, care ulterior sunt supuse aprobarii Comisiei Nationale a Valorilor Mobiliare (Autoritatea de Supraveghere Financiara). - A self-regulatory body, the Bucharest Stock Exchange adopts appropriate rules and procedures, which are subsequently submitted to the National Securities Commission (Financial Supervisory Authority) for approval.

Depozitar central (DC) - Central Depository (CD)

Depozitarul central furnizeaza servicii de compensare, decontare, registru, depozit si custodie pentru valorile mobiliare tranzactionate pe piete reglementate si sisteme alternative de tranzactionare, precum si orice alte operatiuni conexe. - The central depository provides clearing, settlement, registry, depository and custody services for securities traded on regulated markets and alternative trading systems, as well as any other related operations.

Fondul de compensare pentru investitori (FCI) - Investor Compensation Fund (ICF)

Obiectul principal de activitate al Fondului este de a colecta contributii de la membri si de a plati compensatii investitorilor atunci cand un membru nu returneaza banii si / sau instrumentele financiare datorate de investitori sau care apartin acestora, care au fost detinute si / sau gestionate in numele acestora pwentru furnizarea de servicii de investitii, pana la limita de compensare stabilita in conformitate cu regementarile emise de ASF. Toti intermediarii autorizati sa furnizeze servicii de investitii si societatile de administrare a investitiilor care gestioneaza portofolii individuale de investitii trebuie sa fie membri ai fondului. - The main object of activity of the Fund is to collect contributions from members and to pay compensation to investors when a member fails to return money and/or financial instruments owed by or belonging to investors, which have been held and/or managed on their behalf for the provision of investment services, up to the compensation limit established in accordance with the regulations issued by the FSA. All intermediaries authorized to provide investment services and investment management companies managing individual investment portfolios must be members of the fund.

Liquidity analysis of the sector

In the period between 2013-2020, the total capitalization of all companies listed on the regulated market (including at national and international level) fluctuated in the range of 130-180 billion lei, while the value traded as a percentage of the stock market capitalization remained in the range of 5% - 10%. Prior to this period, capital market developments and trading activity were less predictable, with greater fluctuations.

After reaching a record high of 181 billion Ron in 2019, BSE's market capitalization fell by 15% in 2020 (154 billion Ron) as a result of the COVID-19 pandemic.

The market capitalization of the BSE on March 31st, 2021 reached 179 billion Ron, thus recording an annual increase of 16%, while the average monthly traded value in the 1st quarter of 2021 was 20% below the 2020 average.

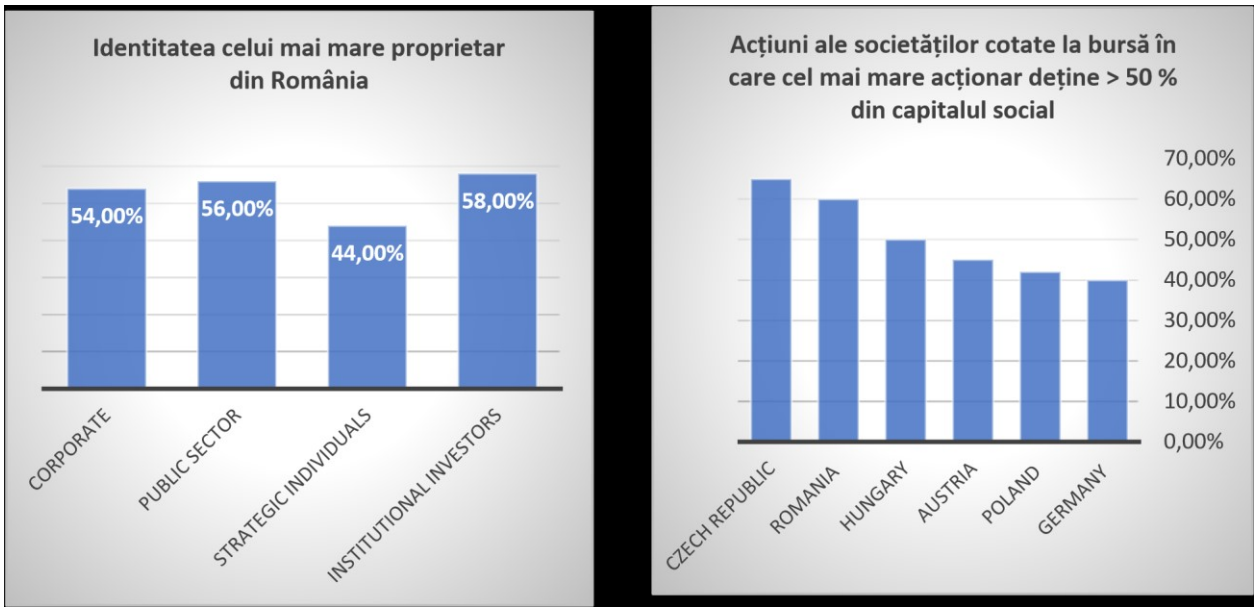
The traded value on the BSE regulated market increased by more than 25% in 2020 compared to the previous year (2020: RON 12.2 billion compared to 2019: RON 9.7 billion). In the last 14 years, the lowest traded value was recorded in 2009 (RON 5.1 billion), when investor confidence was strongly affected by the major corrections in 2008, while the highest level was reached in 2007 (RON 13.8 billion) at the beginning of the financial crisis. The top five most traded shares on the regulated market in 2020 were the same as in recent years, with a total value of RON 8,094,010,996.
Indicators relating to financial instruments and the financial instruments sector (capital market) as at December 31st, 2020:

- The total value traded at the Bucharest Stock Exchange – 18.73 billion Ron[31];
- Total value transacted at the central depository (via a credit institution account): EUR 3.96 million
- Total assets of investment funds in closed-end funds – 41.42 billion Ron;
- Market capitalization at the end of the year 154.37 billion Ron;
- Volume of managed assets, investment firms: EUR 2.362 million;
- Annual turnover of investment firms: EUR 14.57 million;
- Contribution to GDP: 3.92%;
- The volume of assets held by asset management companies: EUR 3.891 million;
- Annual turnover of asset management companies: EUR 21 million.

Market capitalization increased by 40% at the end of November 2021 compared to the end of 2020 and by 19% compared to the end of 2019; in November 2021, the first 3 companies traded on the BSE.

The shareholding structure on the Romanian stock market is quite concentrated. In six out of ten listed companies, the largest single shareholder holds more than 50% of the equity, reflecting a high level of control and concentration. Corporations and holding companies are not only the largest owners at aggregate level, they are also the most widespread shareholders at company level, holding on average 54% of the equity of almost 40% of listed companies. The public sector is also an important owner, but in fewer companies. They own, on average, 56% of listed shares in 17% of listed companies. Institutional investors who are the largest owner in 19% of companies are mainly mutual funds and investment advisors.

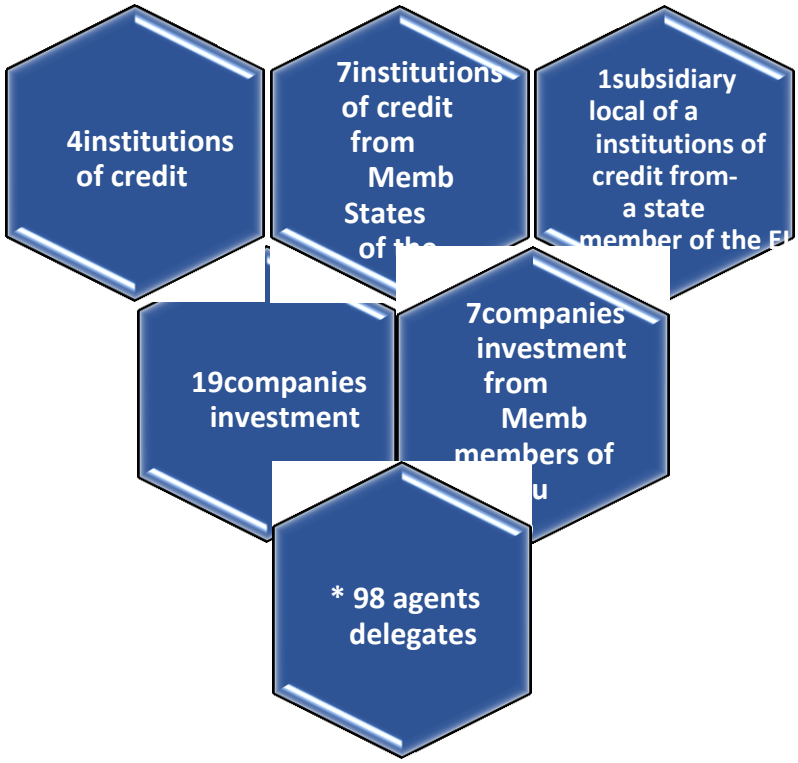
Concentration of control over entities



Identitatea celui mai mare proprietar din Romania - The identity of Romania's largest owner
Actiuni ale societatilor cotate la bursa in care cel mai mare actionar detine peste 50% din capitalul social - Shares of listed companies in which the largest shareholder holds more than 50% of the share capital.

[31] 1 EUR = 4.869 RON

Entities in the financial instruments sector



4 instituii de credit – 4 credit institutions
7 institutii de credit din alte state membre ale UE - 7 credit institutions from other EU Member States
1 sucursala locala a unei institutii de credit dintr-un stat membru al UE – 1 local branch of a credit institution from an EU Member State
19 firme de investitii – 19 investment firms
7 firme de investitii din alte state membre ale UE – 7 investment firms from other EU Member States
**98 agenti delegati - *98 delegated agents*

* An investment agent/delegate who, under the full and unconditional responsibility of a single SSIF on whose behalf he acts, on the basis of an employment, mandate or agency contract, promotes investment services and/or ancillary services to clients or potential clients, receives and transmits instructions or orders from the client regarding investment services or financial instruments, places financial instruments and/or provides advice to clients or potential clients regarding those financial instruments or services.[32]

[32]https://ASFromania.ro/app.php/en/a/1705/registrul-instrumentelor-%C8%99i-investi%C8%9Biilor-financiare

The Collective Investment Fund System (CIS)

115 scheme de plasament colectiv – 115 collective placement schemes
18 societati de administrare a investitiilor – 18 investment management companies
20 societati de administrare a investitiilor din alte state membre – 20 investment management companies from other Member States
66 fonduri deschise de investitii din alte state membre ale UE ale caror unitati de participare sunt distribuite in Romania – 66 open-ended investment funds from other EU Member States whose units are distributed in Romania
10 administratori de fonduri de investitii alternative din alte state membre care isi desfasoara activitatea in Romania – 10 alternative investment fund managers from other Member States operating in Romania
12 societati de investitii din alte state membre ale caror unitati de participare sunt distribuite in Romania - 12 investment companies from other Member States whose units are distributed in Romania

Source: FSA's 2020 annual report

*The open-ended funds of 66 are part of the 115 collective investment schemes

I. Intermediaries of Financial Instruments (SSIF)

In assessing the risk associated with different types of distribution channels to facilitate the provision of securities/financial instruments products and services, intermediaries have been identified as a channel through which securities products and services are distributed and which present a high average risk of being used for money laundering purposes. The majority of intermediaries use investment products and services for their direct clients, where the business relationship is established between the intermediary and the client. Funds received from clients during a business relationship can be transferred using non-bank payment providers and bank accounts opened with an authorized credit institution. Intermediaries who accept the use of non-bank payment providers (a single securities intermediary) are obliged to require that at least one transfer be made to a bank account (IBAN issued by a credit institution). Thus, the use of a credit institution is a sine qua non "tool" that the client should use and prove in order to start a business relationship with an authorized securities intermediary.

Risk analysis and classification included the vulnerabilities identified during off-site and on-site verifications, in addition to the size, nature, type of customer (individuals/legal entities, professionals and retail) and the volume of transactions carried out by intermediaries – legal entities and the following factors were assessed:

- Intermediaries servicing high-risk clients, beneficial owners and their associates without adequate risk mitigation measures;
- Intermediaries with a history of non-compliance with the FSA Regulations;
- Intermediaries who have not attended or completed training/training programs in the field of preventing and combating money laundering and terrorist financing, required by securities providers;
- Intermediaries that have weak internal controls for preventing and combating money laundering and terrorist financing or that have substandard internal compliance mechanisms;
- Intermediaries that do not appoint a person in charge of preventing and combating money laundering and the financing of terrorism (AML/CTF) or that do not comply with the legal framework in terms of preventing and combating money laundering and the financing of terrorism and the remedial measures of the FSA;
- Intermediaries who do not comply with the agreements concluded with securities providers (execution through third parties);
- Intermediaries with a large volume of transactions that have not provided adequate personnel and working tools to fulfill their obligations in the field of preventing and combating money laundering and terrorist financing.

CASE STUDY	
Parties involved:	1. Issuer – joint-stock company listed on the Bucharest Stock Exchange (BSE); 2. Intermediary of financial instruments; 3. Client/bidder – limited liability company;
Operation: offer mandatory public.	During 2020, in the framework of the mandatory public offering of shares (36,816,753 RON) belonging to a joint-stock company listed on the BSE, the intermediary who presented his intention to buy the shares for and on behalf of his client (the new customer) did not take adequate customer precautions. Thus, the intermediary allowed a client associated (through an association agreement) with a criminal (prosecuted in the first instance for, among other things, money laundering offenses) to obtain funds and use them to make the purchase offer of actions. Thus, the client presented to the intermediary the source of the funds as coming from an association (association agreement) with another legal entity (limited liability company), from loans from other limited liability companies owned/controlled by the client of the mandatory public offer, as well as from other own funds. During the execution of the CDD, the intermediary did not verify the client's associate, in fact, the one who was bringing most of the funds to buy the shares. Also, the intermediary did not assess the risk of entering into a business relationship with a customer associated with a criminal, respectively did not assess the origin of the funds and, respectively, the risk of the non-bank financial entity being used for the purpose of money laundering. The situation was assessed by the FSA through the off-site surveillance mechanism and also through a full inspection that covered the topic of ML/TF. Thus, the mandatory public offer made by the intermediary was not approved, and the supervisor issued a fine to the AMLO (AML/CTF compliance officer) appointed for the financial instruments intermediary.

The risk analysis and classification of financial instrument intermediaries also closely assessed the fact that a client/investor may simultaneously have multiple business relationships with different intermediaries.

The risk assessment included the risks associated with the direct commercial relationship between the intermediary and the client. Thus, the risks associated with different types of

clients (publicly exposed persons, criminals and accomplices of criminals, clients from high-risk countries) highlighted the following threats to which financial instruments intermediaries are exposed:

- Publicly exposed persons associated with criminals or involved in criminal activities;
- Clients with professional know-how in the financial instruments sector associated with criminals and/or publicly exposed persons involved in criminal activities;
- Customers who have a non-transparent source of funds or who come from other people involved in criminal activities;
- Customers with a criminal record;
- National and cross-border clients with a complex and non-transparent control structure.

No.	Elements	Likelihood Rating (L)	assessment consequence/impact (C)	Risk level
1.	**Risk**	**High**	**Moderate**	**Medium - High**
Associated vulnerabilities: **For the case mentioned above:** the intermediary did not verify the client's associate, who was in fact a person prosecuted (in the first instance) for, among other things, money laundering offences; The source of the funds was not verified, despite publicly available information; AMLO was not trained to fulfill his anti-money laundering obligations; **Intermediaries of financial instruments at sector level:**				
Intermediaries servicing high-risk clients, beneficial owners and their associates without adequate risk mitigation measures; Intermediaries with a history of non-compliance with the FSA Regulation on AML/CTF; Intermediaries who have not attended or completed training/training programs in the field of prevention and combating money laundering and terrorist financing required by providers of financial instruments; Intermediaries that have weak internal AML/CTF controls or that use substandard internal compliance mechanisms (programs that do not effectively manage compliance with internal policies); Intermediaries that do not designate a person in charge of preventing and combating money laundering and the financing of terrorism (AML/CTF) or that do not comply with the legal framework in terms of preventing and combating money laundering and the financing of terrorism and the remedial measures ordered by the FSA; Intermediaries who do not comply with the agreements concluded with securities providers (execution through third parties); Intermediaries with a large volume of transactions that have not provided adequate staff and working tools to fulfill their obligations in terms of preventing and combating money laundering and terrorist financing;				

Associated threat: **For the specific case mentioned above:** associate of the client, who was in fact a person prosecuted (in the first instance) for, among other things, money laundering offenses – client associate of a criminal who provided the funds used for the public offering; **At the level of securities intermediaries in the sector:** Publicly exposed persons associated with criminals or involved in criminal activities; Clients with professional know-how in the securities sector associated with criminals and/or publicly exposed persons involved in criminal activities; Clients who have a non-transparent source of funds or who present funds originating from other persons involved in criminal activities; Customers with a criminal record; National and cross-border customers with complex and non-transparent control structure;
Event description: The securities intermediary used as a distribution channel to deliver securities products; Possible illicit funds could have been introduced into the securities market by means of a share purchase operation through a securities intermediary, thus, with the apparent aim of buying a block of shares in a public company, a criminal (pursued at first instance) attempted to use funds to acquire ownership of a listed company;
Risk description: Placement of possible illicit funds on the securities market with the help of an intermediary (non-banking financial institution)

When assessing the residual risk associated with the activity of financial instruments intermediaries, respectively when assessing the risks after the application of mitigation measures, it was found that financial instruments intermediaries present an average residual risk of being used for the purpose of money laundering.

II. Investment agents/delegates

When assessing the risk associated with different types of distribution channels to facilitate the provision of securities products and services, investment agents/delegates were identified as a medium risk channel through which securities products and services are distributed to be used for money laundering purposes.

The risk analysis and classification of investment agents/delegates acting under the full and unconditional responsibility of a single investment firm on whose behalf they act included the vulnerabilities identified during supervision, taking into account the following factors:

- Failure of the investment firm to organize mandatory training/training programs in the field of preventing and combating money laundering and terrorist financing for mandated delegated agents;
- Failure to establish through a mandate the obligations of the exact delegated agents in the matter of preventing and combating money laundering and the financing of terrorism;
- Deficiencies identified in internal policies/procedures applicable to delegated agents.

The risk assessment included the risks associated with the direct commercial relationship between the delegated agent and the client. Thus, the risks associated with different types of clients (publicly exposed persons, criminals and accomplices of criminals, clients from high-risk countries) revealed the following threats to which the delegated agent may expose the investment firm under whose responsibility it acts:

- Publicly exposed persons associated with criminals;

- Clients with professional know-how in the securities sector associated with criminals and/or publicly exposed persons;
- Customers who have a non-transparent source of funds or who come from other people;
- Customers with a criminal record;
- Resident and cross-border customers with non-transparent ownership.

No.	Elements	Probability assessment	assessment consequences/impact	Risk level
1.	Risk	high	moderate	average
Associated vulnerabilities: **Failure of the investment firm to organize mandatory training/training programs in the field of preventing and combating money laundering and terrorist financing for mandated delegated agents;** **Failure to establish through a mandate the exact obligations of the delegated agents in the matter of combating money laundering and the financing of terrorism;** **Deficiencies identified in internal policies/procedures applicable to delegated agents;**				
The delegated agent does not properly carry out customer due diligence, proper verification of the source of funds used by customers;				
Associated threat: **Publicly exposed persons associated with criminals;** **Clients with know-how in the securities sector associated with criminals and/or publicly exposed persons;** **Customers who have a non-transparent source of funds or who come from other people; Customers with a criminal record;** **Resident and cross-border customers with non-transparent ownership; Customers with criminal experience, publicly exposed persons associated with criminals;**				
Event description: **Delegated agents receive and transmit instructions or orders from clients using funds from potentially illicit sources to purchase financial instruments (securities).**				
Risk description: **Placement of possible illicit funds on the securities market through an intermediary of financial instruments, respectively a natural person - under the full and unconditional responsibility of a single intermediary (SSIF) or on whose behalf he acts on the basis of an employment contract, a mandate or of an agent contract, promotes investment services and/or ancillary services to clients or potential clients;**				

When assessing the residual risk associated with the activity of delegated agents, respectively when assessing risks after the application of mitigation measures, it was found that this type of investment agents/delegates presents an average residual risk of being used for the purpose of money laundering.

III. Providers of Financial Instruments (investment management companies, alternative investment management companies, investment companies, Fondul Proprietatea)

When assessing the risk associated with the activity of managing investment funds (open-end and closed-end investment funds), it was found that this type of non-banking financial institutions that provide products and services in the field of securities as part of a commercial activity presents a risk medium to be used for money laundering purposes.

The risk analysis and classification of financial instrument providers included, in particular, the fact that collective investment products are made in a non-monetary way, i.e. using only bank accounts managed by credit institutions. In addition, in addition to the size, nature,

clients, source and use of funds, the volume of transactions and the following vulnerabilities were identified in the course of supervision and taken into account:

- Transactions executed on behalf of another person;
- Transactions executed in a non-transparent manner;
- Transfer of securities between entities in different countries;
- Accepting funds from high-risk or sanctioned countries;
- Clients with non-transparent ownership structures, sophisticated systems and clients with a large volume of funds, the origin of which is not clear;
- Deficient internal preventive controls and deficient mitigating measures.

Securities products and services are usually distributed directly to customers (including online) or through intermediaries. Securities providers that distribute securities products and services through online channels, through securities intermediaries, have been identified as having the following vulnerabilities:

- Failure to carry out a risk assessment of the online channel thus used, without preventing the risk of being used for money laundering purposes;
- Deficiencies in customer due diligence with respect to the customer and also the beneficial owner or person controlling it due to the non-transparent ownership mechanism;
- Failure to conduct adequate training with securities intermediaries (recourse to third parties) regarding customer precautions;
- Non-verification of information collected by intermediaries directly from the client; relying solely on the intermediary's customer due diligence;
- The designated AMLO (AML/CTF compliance officer) does not have the appropriate professional skills to coordinate preventive internal control measures in the field of preventing and combating money laundering and terrorist financing;
- Lack of internally implemented controls to comply with the market abuse legal framework;
- Lack of oversight of trading activity to monitor any suspicious activity for the purpose of preventing and control of money laundering.

Providers of financial instruments range from those that interact heavily with retail investors, such as retail brokers, wealth managers and financial advisors, to those that serve a largely institutional market, such as clearing members, prime brokers, global custodians, sub-custodians and custodian banks, including securities depository participants. Some of the largest securities providers operate through different legal divisions or entities within the same group (credit institutions alongside non-bank financial institutions[33]).

The risk assessment is completed by the threats to which securities providers are exposed:

- Criminals accepted as clients by an intermediary, thereby accepting the use of illegal funds to purchase securities;
- Offenders as direct clients of the securities provider;
- Publicly exposed persons associated with criminals or with criminal involvement;
- Group of investment professionals acting together and using a person as a client of the investment company;

[33]For example, SAI Wood &Company (Wood &Company), BRD Asset (BRD Group)

- legal entity whose ownership structure is unreasonably complex and has a non-transparent ownership structure;
- A securities provider that acts as an intermediary or otherwise, but is either unregulated or regulated in a jurisdiction with weak anti-money laundering and countering the financing of terrorism oversight;
- Intermediaries suspected of committing crimes, especially financial crimes or association with criminals.

No.	Elements	Probability assessment	assessment consequences/impact	Risk rating
1.	**Risk**	**High**	**Moderate**	**Average**

Associated vulnerabilities:
Transactions executed on behalf of another person;
Transactions executed in a non-transparent manner;
Transfer of securities between entities in different countries;
Accepting funds from high-risk or sanctioned countries;
Clients with non-transparent ownership structures, sophisticated systems and clients with a large volume of funds, the origin of which is not clear;
Deficient internal preventive controls and deficient mitigation measures;
Failure to carry out a risk assessment of the online channel thus used, without preventing the risk of being used for money laundering purposes;
Deficiencies in customer due diligence with respect to the customer and also the beneficial owner or person controlling it due to the non-transparent ownership mechanism;
Failure to conduct adequate training/training with securities intermediaries (recourse to third parties) regarding customer precautions;
Non-verification of information collected by intermediaries directly from the client; relying solely on the intermediary's customer due diligence;
The appointed AMLO (anti-money laundering compliance officer) does not meet the appropriate professional competences to coordinate preventive internal control measures in the field of combating money laundering and terrorist financing;
Lack of internal controls implemented to comply with the legal framework on market abuse;
Lack of oversight of trading activity to monitor any suspicious activity for the purpose of combating money laundering;
Failure to conduct an independent annual anti-money laundering audit;
Failure to report suspicious activity identified upon opening a business relationship.

Associated threat:
Criminals accepted as clients by an intermediary, thereby accepting illicit funds
to be used for the purchase of securities; Offenders as direct clients of the securities provider;
Publicly exposed persons associated with criminals or with criminal involvement;
Group of investment professionals acting together and using a person as a client of the investment company;
A legal entity whose ownership structure is unreasonably complex and has a non-transparent ownership structure;

A securities provider that acts as an intermediary or otherwise, but is either unregulated or regulated in a jurisdiction with weak AML/CTF oversight;
Intermediaries suspected of criminal activities, especially financial crimes or association with criminal associations.

Event description: Illicit funds (including those from market abuse crimes as a predicate offense) brought by a client associated with other securities professionals and/or criminals, presented as a source of funds for investment purposes.
Risk description: Illicit funds are transferred through a bank account to an asset management company that puts the capital to work through various investments, including stocks, bonds, real estate. SAI can therefore create common structures such as mutual funds or ETFs (exchange traded funds) that they can manage in one centralized portfolio. Thus, illicit funds are placed in investments on the capital market.

When assessing the residual risk associated with the management of collective investment funds (open-end and closed-end investment funds), respectively when assessing the risks after the application of mitigation measures, it was found that investment fund management companies present an average risk residual to be used for the purpose of money laundering.

IV. Investment funds (open-end investment funds and closed-end investment funds)

When assessing the risk associated with the activity of investment funds (open-end and closed-end investment funds), it was found that this type of non-banking financial products presents an average risk of being used for the purpose of money laundering by an asset manager. For more details, see the references mentioned above in relation to the activity of managing investment funds.

The assessed residual risk associated with investment funds is presented in the section mentioned above, which deals with the activity of managing investment funds.

V. Custodians of financial instruments (custody/custody entities)

Custodians of financial instruments (depositories/custodian institutions) are credit institutions that ensure the safe custody of all investment fund assets (cash, securities and other investment assets), the settlement of securities transactions on behalf of the securities provider (investment companies, asset management companies), the collection of dividends, interest and other benefits related to the deposited assets, and the exercise of the rights conferred by these assets, in accordance with the instructions received from the asset management companies; the receipt of funds for the subscription of units of open-ended investment funds and shares of investment companies and the processing and issuing of such securities and the processing of redemption requests for open-ended investment funds, the cancellation of securities and the making of corresponding payments to holders.

Thus, due to the fact that these financial institutions act (receive and transfer funds) based on the orders of the securities provider, it was found that depository and custody financial institutions present a medium risk of being used for money laundering purposes in the financial sector non-bank

The risk analysis took into account the assessment of the vulnerabilities of the operations carried out by the financial institutions acting as custodians for the securities providers, such as:

Execution of orders, other than those received directly from financial instrument providers, thus effecting an unauthorized transfer of funds.

No.	Elements	Probability Rating (P)	assessment consequences/impact (C)	Risk level
1.	**Risk**	**Low**	**Moderate**	**Average**
Associated vulnerabilities: Making a transfer of funds to the customer's order, which is not based on the direct order of the securities provider.				
Associated threat: Customers with a criminal background or involved in criminal activities, even in relation to criminals Publicly exposed persons associated with criminals.				
Event description: The customer involved in criminal activities directly requests the custodian to suddenly and immediately transfer the funds, and the custodian does not comply with the legal requirements and accepts the transfer.				
Risk description: Unauthorized funds are transferred directly to the customer involved in criminal activities.				

When assessing the residual risk associated with the activity of a credit institution authorized as a depository or custodian of securities, respectively when assessing the risks after the application of mitigation measures, it was found that depositories of financial instruments present an average residual risk of being used for laundering purposes of money.

INVESTMENT PRODUCTS AND SERVICES (FINANCIAL INSTRUMENTS)

In the overall risk analysis of the investment products and services provided to clients/investors, the following attributes indicating a higher risk were identified:

- any unusual complexity or structure, without obvious economic purpose;
- Omnibus account services, due to the inherent favoring of anonymity or obscure information regarding the underlying transaction with customers;
- securities at low prices that have been subject to market fraud and abuse;
- the use of new payment technologies or methods that are not used in the normal course of business by securities providers (payment service providers authorized in other EU countries or high-risk jurisdictions).

The financial instruments mainly traded on the securities market are undoubtedly shares, structured products and corporate bonds, as follows: Structure of BVB transactions (BVB and SMT market) by value and number of transactions for each type of financial instrument

Type of products	31.12.2019			31.12.2020			Variations	
	No. of trans.	Value (lei)	%	No. of trans.	Value (lei)	%	No. of trans.	Value
Shares	512,807	9,910,960,145	81.54 %	836,141	12,572,185,291	67.14%	63.05%	26.85%
Bonds, inclusive EURBONDS, EUR-TBILLS and EUR-TBONDS	6,218	2,047,364,629	16.84 %	18,722	2,632,525,706	14.06%	201.09%	28.58%

Structured products (warrants and certificates)	56,861	185,899,982	1.53%	108,992	828,795,845	4.43%	91.68%	345.83%
Government bonds	91	4,090,043	0.03 %	19,435	2,677,927,575	14.30%	21257.14 %	65374.3 2 %
Unity background	2,719	7,017,125	0.06 %	6,195	14,419,761	0.08%	127.84%	105.78%
Total	578,696	12,155,331,923	100%	989,485	18,725,874,178	100%	70.99%	54.05%
Total (Euros)	—	2,480,679,984	—	—	3,821,606,975	—	—	—

*BVB source

Evolution of total assets by category of mutual funds of collective investment schemes with transferable securities (UCITS) (millions of RON)

fund	**Total assets 31.12.2019**	**Total assets 31.12.2020**
Undertakings for collective investment in traded securities	22,522	19,677
Alternative investment fund	1,601	1,479
Investment firm	11,921	10,322
The Proprietatea Fund (FP)[34]	10,524	9,944
TOTAL	46,568	41,422

*FSA 2021 report source

The global risk analysis of the financial instruments (capital market) sector, taking into account the volume of traded funds, the vulnerabilities and threats identified within the supervisory mechanism used (both proactive and reactive), revealed an average inherent risk and a residual environment.

VI. Administrators of optional pension funds, a single administrator of occupational pension funds (authorized on February 9th, 2022)

When assessing the risk associated with the activity of managing voluntary pension funds, it was found that non-bank financial institutions, respectively companies that manage voluntary pension funds, especially due to the characteristics of the managed product, present a low risk of being used for money laundering purposes.

The risk analysis and classification of optional pension administrators included an assessment of the distributed product, in particular the specific characteristic of the fact that it is a product that reaches maturity only at the moment of compliance with the legal retirement

[34]PF as in the case of the asset manager of open-ended investment funds and alternative investment funds

conditions or at the moment of biometric risks (disability, death - case where accumulated funds are transferred to legal heirs).

Thus, the client of a voluntary pension system does not benefit from accumulated funds until retirement (age 60) and in case of disability (or at least 90 accumulated contributions). In addition, the contribution to a voluntary pension fund can be up to 15% of gross monthly income or salary equivalent.

In addition to the risk classification features mentioned above, only the following vulnerabilities were identified within the surveillance mechanism:

- deficiencies in the internal control policies/procedures issued by the management of the regulated entity, respectively technical compliance deficiency.

No.	Elements	Probability Rating (P)	assessment consequences/impact (C)	Risk level
1.	**Risk**	**Low**	**Low**	**Low**
Associated vulnerabilities: Internal procedures do not fully provide for the rules set out in the sectoral legal framework on preventing and combating money laundering – technical vulnerability in terms of compliance.				
Associated threat: Optional private pension systems are savings and investment instruments intended to be accessed only at maturity, i.e. at the client's retirement age (60 years) or in case of biometric risks.				
Event description: due to deficiencies in internal policies/procedures issued by the pension company, a client provides more than 15% of gross monthly income or salary equivalent and there is no red flag implemented at the level of the business relationship monitoring mechanism of administrator or any precautions that need to be taken.				
Risk description: The illicit funds are placed in a savings product, i.e. an optional private pension scheme that can be accessed at retirement age, in case of disability or by the clients' heirs in the event of the clients' death.				

The analysis of the overall level of risk of voluntary private pension products, taking into account the characteristics of the products, the vulnerabilities and the threats identified within the supervisory mechanism used (both proactive and reactive), revealed a low risk and a low residual risk after application of mitigation measures.

Elements of the risk-based approach implemented by FSA in the financial instruments/capital market sector.

The Strategy/Risk Model of the FSA takes into account elements of a prudential nature which are complemented by specific elements of ML/TF (money laundering/terrorist financing) by the specialists of the specialized structure of the FSA, all of which are taken into account when establishing measures to address the risks involved, as well as the frequency and complexity of controls (including actions to monitor the remediation of the identified deficiency) on the activities of entities on the capital market (financial instruments sector).
The sectoral mechanism provides for the identification of risks taking into account all the specific elements of the products and services offered by entities on the capital market, as well as the architecture of the entities (including the group they belong to, if applicable), quantifying the risks identified and evaluating them in order to determine the risk class at entity and sector level. Within the sector-wide risk-based supervisory mechanism, warning measures (alert signals/alerts) are also put in place for entities that present risks that could place them in a whistleblowing zone.

Thus, the sectoral risk assessment mechanism is a first line of analysis that consists of:

- The first stage consists of an initial risk identification and an ongoing risk identification through:
  - their quantification/assessment in a specific way, to allow consideration of both the probability of the occurrence of the event and its impact;
  - recording assessments/quantification in a clear way that allows monitoring;
  - making a separation between inherent risk and residual risk;
- The second stage, the risk approach as a stage of risk management through mitigating/remedial measures through: o preventive measures o corrective measures; o directive measures; o detective measures.

In situations where the identified, quantified and evaluated risks present elements specific to the early warning area, reporting to the independent structure with a ML/TF prevention profile takes place (second line of analysis).

The stage of the second segment of the experts' analysis deepens the specific elements/activities of ML/TF, complementary to the specific elements of prudential sectoral supervision, and takes into account the following factors necessary for the assessment of inherent risks at the level of supervised entities:

- The risks associated with the entity authorized to carry out trading activities with financial instruments,
- Risks associated with customers;
- The risk associated with the geographical area (jurisdiction);
- The risk associated with the product or service provided;
- The risk associated with the distribution channel;
- The risk associated with the transaction.

All elements of prudential supervision and conduct, complemented by elements of ML/TF, form the basis of ML/TF assessment at the entity/sector level and generate annual risk reports on the threats and vulnerabilities to which the entity/sector is exposed, factor mapping of risk, as well as supervisory measures to address and mitigate exposure to the risk of money laundering or terrorist financing and monitoring processes (addressing identified risks).

The annual risk reports provide a classification of non-banking financial entities by risk categories and measures to address identified and quantified risks, i.e. measures that will materialize in the type of inspection (full scope, thematic procedure, ad hoc, consolidated monitoring) and the frequency of inspections, the results of which will determine the effective measures to be taken to address the threats to which the entity is exposed and to mitigate or remedy its vulnerabilities.

These elements are taken into account in the annual control plan and determine the frequency of inspections.

The specialized structure at the level of the capital market supervision mechanism determines the type of entities, depending on the risk profile resulting from the assessment of sectoral risks, and these are subjected to the ML/TF analysis by the specialists of the specialized structure, who determine the vulnerabilities of the entity, as well as the threats ML/TF to which it is exposed.

Sectoral risk assessments, supplemented by risk assessments from a ML/TF perspective, form the basis for the development of the annual inspection plan, which can be modified at any time of the year depending on the risk events that occur/are likely to occur/materialize.

Risk events that have arisen and been identified with the help of proactive financial entity monitoring tools may lead to an ad hoc inspection of specific entities or activities or may constitute grounds for triggering hearings at the FSA headquarters.

Thus, in proportion to the risk class of the supervised entity, as well as to the characteristics/nature of the entity (investment firm, investment manager, intermediary, etc.) thematic inspections, substantive inspections and ad hoc inspections, the following must be taken into account:

- Elements of compliance with the obligations provided for in the legal framework of the FSA:
  - the measures and control mechanisms put in place at the entity level to manage and mitigate money laundering or terrorist financing threats;
  - the effectiveness of the preventive control mechanisms implemented, as well as the allocated resources;
  - the ability of the financial entity to address and mitigate the ML/TF threats to which it is exposed;
- the measures taken to remedy the deficiencies identified and included in the remedial plan following the previous inspections carried out by the FSA.

Inspection results are classified as insignificant, significant and serious violations identified and taking into account their impact on the integrity of the non-banking financial sector.

At the level of financial entities that trade financial instruments (securities sector), the following violations or deficiencies (ML/TF vulnerabilities) have been identified:

- Failure to appoint a person in charge of preventing and combating money laundering who meets all the conditions of competence and integrity necessary to manage ML/TF threats and vulnerabilities in the financial entity's activity and/or business relationships;
- deficiencies identified at the level of preventive measures/internal control mechanisms implemented at entity level, namely:
  - deficient elaboration of the internal customer due diligence procedures; o insufficient knowledge of the clientele;
  - the lack of a money laundering or terrorist financing risk assessment or the existence at the entity level of an outdated money laundering or terrorist financing risk assessment;
  - lack of documentation of money laundering/terrorist financing risk assessments carried out at the level of the entity's activity and, individually, at the level of business relationships/occasional transactions;
  - lack of continuous monitoring of high-risk factors for money laundering or terrorist financing (taking into account the volume of transactions, type of customer, product, service, distribution channel or geographical area);
  - lack of identification and documentation or superficial documentation of the customer's beneficial owner;
  - failure to report suspicious activities or transactions to FIU (STR);

- o failure to carry out an independent ML/FT audit to test the effectiveness of the preventive internal control measures implemented;
- o lack of training/instruction of personnel with responsibilities in matters of money laundering or terrorist financing (front office or persons directly related to the client, persons who analyze and approve the opening or termination of a business relationship).

Violations and deficiencies identified during inspections of financial entities on the capital market (substantive, thematic or ad hoc) are generally due to the following vulnerabilities:

- lack of money laundering or terrorist financing training of staff of the supervised non-banking financial entity;
- limited access to beneficial ownership information, both nationally and internationally;
- Insufficient resources to cover obligations to prevent and combat money laundering or terrorist financing.

When assessing the appropriate and proportionate level of remedial measures and sanctions imposed on financial entities, the following shall be taken into account:

- the nature of the findings/deficiencies regarding the higher risk elements identified in the system/sector of entities that trade financial instruments;
- the impact of the identified deficiency with respect to the entity's exposure to the entity to the non-banking financial sector/financial system;
- the use of available sanctions, including withdrawal of authorization/licence to operate;
- publishing information on sanctions imposed on an entity in order to inform all entities in the sector so that they are aware of the necessary measures to address similar risks.

In addition to the sanctions imposed on the entities that are the subject of the inspection or independently of any sanction imposed, FSA also develops plans with measures to remedy the identified deficiencies, the follow-up of which is subject to monitoring at the supervisor's headquarters with a view to their full implementation and efficient by the financial institution.

The supervision (inspection and monitoring) of entities in the financial instruments and investments sector, depending on the type of entity and financial instrument(s), identified in the period 2017-2020, presented the following money laundering or financing threats of terrorism:

- Non-transparent PEP clients (namely refusal to disclose information regarding the source of funds used and the actual beneficiary);
- Non-resident clients/investors, from geographical areas identified as being included in the short list of FATF standards;
- Convicted (at first instance in court proceedings) of, among other things, money laundering;
- Clients who are legal entities with links to organized criminal groups from other EU member states;
- Non-transparent and non-transparent virtual assets (in terms of customer identity and source of funds).

Supervised Non-Banking Financial Entities – Money Laundering/Terrorist Financing Risk Factors/Perception Assessment and Money Laundering/Terrorist Financing Risk Analysis

Given the application of the Council of Europe's National ML/TF Risk Assessment methodology to entities in the financial instruments and investments sector, especially investment management companies[35] (SAI), investment management service companies (SSIF) and systemically important institutions – Bucharest Stock Exchange and the central depository, 91.91% of the entities responded to the questionnaire. A total of 39 capital market entities responded to the questionnaire.

The questionnaires were communicated to financial entities through the professional associations they belong to, as well as directly to entities that are not members of an association, namely the Bucharest Stock Exchange and the Central Depository. Subsequently, two returns were requested for the detail and granularity of certain information, as well as for the deepening of certain elements of interest in relation to the issues raised in the analytical work.

Processing of questionnaire responses reveals a medium awareness of the risks of money laundering and terrorist financing, with an increased focus on money laundering. Regarding the direct obligations of the entities, there is a good knowledge of the legal provisions and guidelines on money laundering or terrorist financing risk factors and various issues have been raised (the high cost of database queries, the low number of training courses accessible to the entity's staff, the need for feedback from financial intelligence units on current money laundering or terrorist financing typologies).

Following the completion of the responses, there is a common cross-sectoral position on the perception that the source of money laundering arising from domestic crimes is tax evasion[36], corruption[37] and organized crime[38]. The cross-sectoral common position on the perception of the source of money laundering arising from external crimes refers to organized crime[39], tax evasion[40], human trafficking[41] and drug trafficking[42], as well as the share of external crimes provided for money laundering.

It is noted that the majority of NBFIs perceive that external sources of income that can be subject to money laundering are predominant in Romania, which also explains the option of being a jurisdiction used for the placement of money. Thus, there is a majority position for this main stage of the crime of money laundering, compared to the other two variants, stratification[43] and integration, in[44] which there are different cross-sector positions, as a total weight, and therefore it is financial sectors that have mostly opted for stratification, while other sectors have opted for integration as the second majority stage.

[35]Of which 3 SIF and Fondul Proprietatea

[36]SSIF 82.2%

[37]SSIF 53.47%

[38]SSIF 32.8%

[39]SSIF 68.85%

[40]SSIF 52.83%

[41]SSIF 44.9%

[42]SSIF 43.63%

[43] 40% of fund management companies and financial investment services companies

[44]one third of investment and fund management companies

The general reasons for filing a suspicious transaction report with the NOPCML are:

- Incomplete information on the real beneficiary of the funds;
- Lack of an economic reason for the transaction[45];
- Negative media information about the client[46], suspicions about the source of the funds[47], suspicions regarding the real beneficiaries[48] and involvement in cases of corruption (giving or taking bribes), foreign transfers from a jurisdiction other than the residence of the beneficial owner, high-risk clients (PEPs);
- The value[49]of the transaction in relation to the source of the funds.

Specific legislation (KYC, CDD) is considered the most useful legal or methodological tool in the field of preventing and combating money laundering and terrorist financing.

Asset management companies have a high level of awareness of several preventive measures that need to be improved, such as:

- Available and transparent information about the beneficial owner;
- Placement of clients in risk groups;
- Informing authorities with powers to identify suspicious money laundering/money generating operations;
- Training;
- Customer information forms;
- Statistical reporting to financial information units;
- National electronic databases/registries/lists of terrorist individuals and entities;
- Updated certificates from commercial registers;
- Financial investment services companies have also added the following crackdowns: Available and transparent information on the beneficial owner;
- Limiting the use of cash;
- Assess policies and procedures to prevent and combat money laundering and terrorist financing;
- Applications based on artificial intelligence (AI);
- • Identification of publicly exposed persons (PEP).

4.3.3. INSURANCE - REINSURANCE SECTOR

General description

Indicators for the insurance and reinsurance sector as of December 31st, 2020:

- Gross written premiums (PBS): 11.5 billion RON;
- Insurance penetration rate in GDP: 1.17%;
- Gross technical reserves for general insurance (AG): 10.5 billion lei;
- Life insurance gross technical reserves: 8.4 billion lei;
- Total volume of assets under management: EUR 6.094 million

[45]Investment management companies 42.85%, financial investment companies 26.64%, Bucharest Stock Exchange and central depository 50%

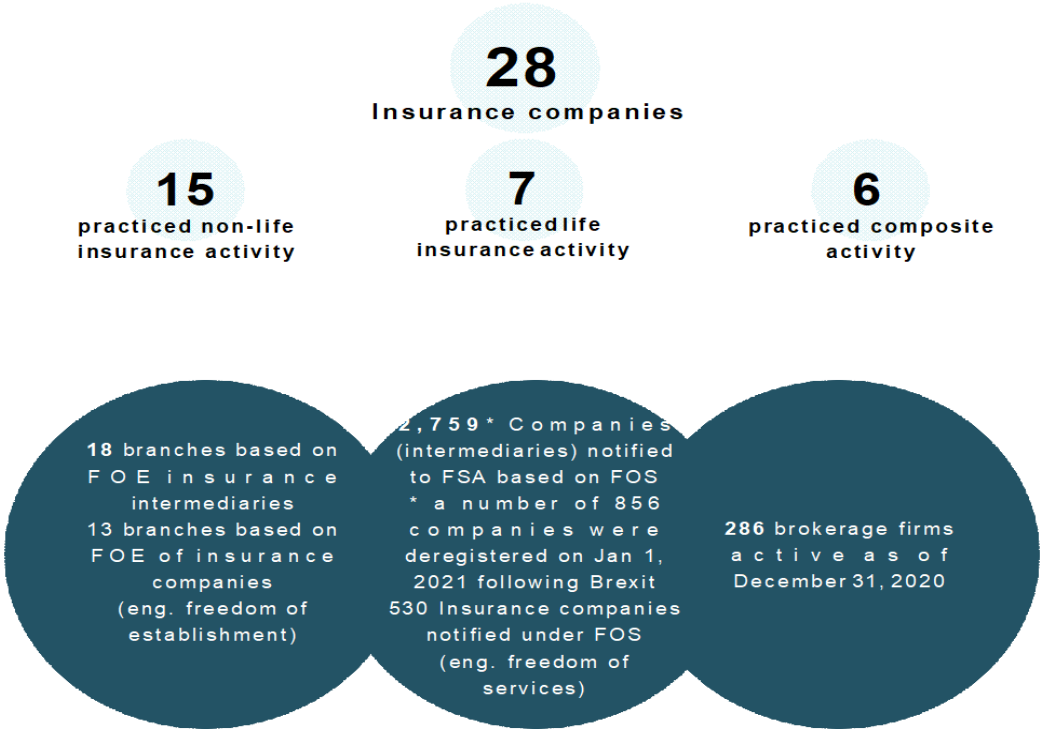
[46]Asset management companies

[47]Asset management companies about 5%, asset management companies 26.64%

[48]Asset management companies approximately 5%, financial investment services.3%;

[49]Investment management companies 42.85%, financial investment companies 26.64%, Bucharest Stock Exchange and central depository 50%

- Annual turnover: EUR 835 million
- Contribution to GDP: EUR 1230 million (2.25%);
- The total volume of assets under management of life insurance companies (LA): EUR 1,890 million;
- Annual turnover of life insurance companies: EUR 203 million
- Contribution of life insurance companies to GDP: EUR 221 million;
- Insurance companies: 26 insurance companies operated on the insurance market, authorized and regulated by the FSA, of which 13 only carried out general insurance activities ("AG"), 7 only carried out life insurance activities ("AV") and 6 were engaged in mixed activities (September 30, 2021).



Evolution of the volume of gross written premiums (lei):

	2016	2017	2018	2019	2020
AG	7,711,487,926	7,688,478,353	8,042,071,138	8,734,210,208	9,275,618,436
AV	1,669,447,247	2,013,265,250	2,102,455,293	2,256,015,186	2,219,296,835
IN THE OVERVIEW	9,380,935,173	9,701,743,603	10,144,526,431	10,990,225,394	11,494,915,271
AG (%)	82%	79%	79%	79%	81%
AV (%)	18%	21%	21%	21%	19%

Evolution of gross claims paid, including maturity and redemptions for non-life (AG) and life (AV):

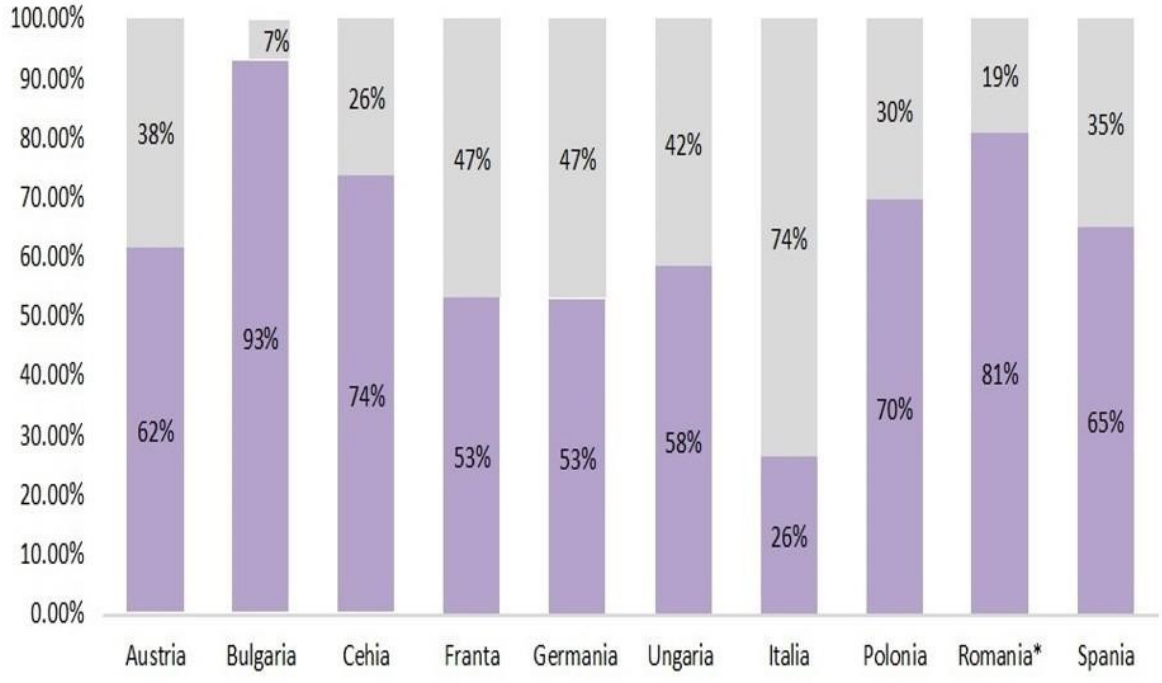
year	PBI AG + AV (lei)	PBI AG (RON)	PBI AV, maturities, total and partial redemptions (RON)
2016	4,311,825,389	3,601,564,195	710,261,194
2017	5,075,341,698	4,076,896,562	998,445,136

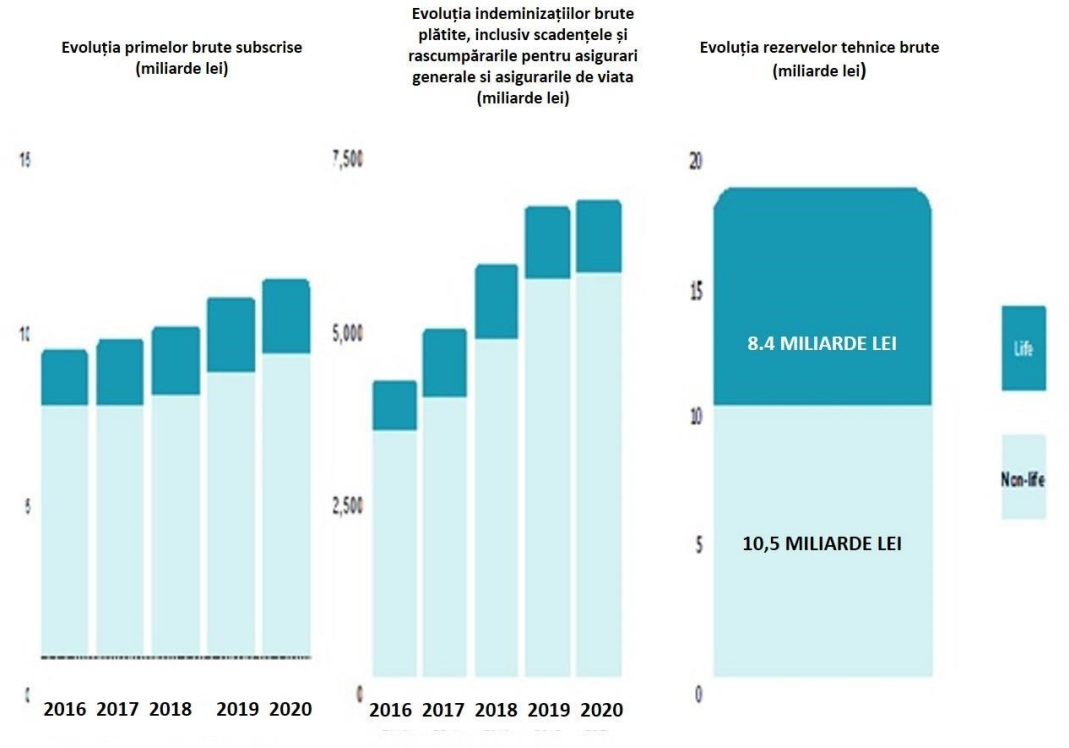
2018	5,957,011,869	4,930,614,341	1,026,397,528
2019	6,827,117,471	5,769,804,707	1,057,312,764
2020	6,949,379,278	5,866,391,603	1,082,987,675

Figura 9 Evoluția volumului de prime brute subscrise în perioada 2016 – 2020

Tabelul 4 Dinamica repartizării pe segmente de asigurare în perioada 2016 – 2020

Structura pieţei asigurărilor în funcţie de primele brute subscrise pentru activitatea de asigurări generale, respectiv de viaţă (Trim. III 2020)





Liquidity of the sector

The liquidity ratio is determined as the ratio between the liquid assets required by the rules and the insurers' short-term obligations towards the insured. In accordance with prudential requirements, its value must be above unity. On December 31, 2020, the liquidity ratio for each category of insurance and the elements that contributed to its formation were as follows:

Table: Liquidity coefficient for each category of insurance as of December 31st, 2020

	State titles (million lei)	Bonds Municipal (million lei)	Securities traded (mil. lei)	Deposits (million lei)	Current account and record (mil. lei)	Short term obligations (million lei)	coefficients net of liquidity e
AG	5,329	27	374	454	912	2,982	2.38
AV	4,616	64	1,457	163	189	1,393	4.66

For the life insurance activity, on December 31st, 2020, insurance companies constituted gross technical provisions in the amount of 8,402,851,485 lei (1.867 billion EUR), of which class C1, Life insurance, annuities and additional life insurance, and class C3, Life and Annuities related to investment funds, together represent approximately 98.82% of the total.

With regards to stability, the total value of gross technical provisions established by insurance companies was at a level of over 18 billion lei, up by 6% compared to the end of 2019 (17,825,299,639 lei). Of the total value of gross technical provisions, 55% represent provisions set up for general insurance, while 45% of the total technical provisions are set

up for life insurance. The surplus of assets over liabilities was approximately 6 billion lei on December 31st, 2020, increasing by 12% compared to 2019.

General risk analysis in the Insurance - Reinsurance sector

The risk assessment applied at the level of the insurance-reinsurance sector from a prudential perspective and supplemented with elements of money laundering/terrorist financing takes into account the volume of premiums earned, the type of insurance entity (insurance company or insurance intermediary), the categories of customers (residents, non-residents, PEPs) with whom business relations are concluded, the products and services provided and their distribution channels.

All reporting entities, including life insurers, are required to carry out an assessment of the risk of money laundering or terrorist financing at the entity level, to have policies and mechanisms in place to assess and mitigate this risk, and to have testing procedures, including audit procedures. In relation to their customers, entities shall be required to know their customers and apply appropriate customer due diligence measures, identify the beneficial owner and monitor the business relationship and, depending on the information obtained, the products accessed and the manner in which the transaction is carried out, and other elements set out in the customer acceptance policy, the entity shall determine the risk category of the customer under conditions that allow for the demonstration of inclusion in a particular risk category. All this information is kept for 5 years or more in exceptional cases. The internal anti-money laundering and anti-terrorist financing policy sets out the requirements for obtaining information at the establishment of the business relationship and also at the time of payment (legal obligation). During the contract, the frequency of screening is determined according to the level of risk. All elements used in the ML/TF risk strategy are taken into account when determining the frequency and complexity of checks (including subsequent actions to remedy identified deficiencies) on the activity of entities in the insurance sector (life insurance, investment insurance and composite insurance).

Life insurance policies are distributed by the resident insurer/branch or by an insurance intermediary (insurance broker), which is also a reporting entity and applies know-your-customer measures for customers proportionate to the risk associated with the relationship and in accordance with the provisions of EU Directive 2015/849. Customer classification and monitoring measures also generate a risk mitigation factor.

Thus, since most of the gross life insurance premium, as a product offered by Romanian insurers, is paid only in the event of a predetermined event, such as death, or on a certain date, as in the case of credit life insurance policies covering loans, consumption and mortgages, which are paid only on the death of the insured person, it results in a low ML/TF risk factor of the product.

Thus, the risk strategy applied to the insurance-reinsurance sector from a prudential perspective and complemented with money laundering/terrorist financing elements takes into account the volume of premiums earned, the type of insurance entity (insurance company or intermediary), the categories of customers (resident, non-resident, PEP) with whom business relationships are concluded, the products and services provided and their distribution channels.

Currently, the FSA carries out controls at the premises of insurance companies and insurance intermediaries with specialized staff assigned to the sectoral supervisory

mechanism, but uses joint supervisory teams (specialists in the field and in the field of anti-money laundering), so that, where appropriate, specialists from the independent structure of the ML/TF, with responsibilities for analysis and supervision/monitoring of non-banking financial entities, can also participate in addressing money laundering or terrorist financing risks.

The annual reports present a classification of entities according to risk category as well as the measures to address the identified and quantified risks, i.e. the measures that will materialize in the type of inspection (substantive, thematic, ad-hoc, continuous monitoring) and the frequency of inspections, the results of which will define the actual measures to be taken to address the threats to which the entity is exposed and to mitigate or remediate its vulnerabilities. From this, the FSA establishes the annual control plan for entities carrying out insurance activities based on a methodology, the action plan itself being a measure to address the risks assessed at sector level, in which specialists in preventing and combating money laundering may also participate. Risk events that have arisen and have been identified using the proactive tools for monitoring financial entities may lead to ad hoc controls of specific entities or activities or may be grounds for triggering hearings at the FSA's headquarters.

The first step in the supervisory process is the quarterly assessment and classification of companies according to their risks and impact on the insurance market. The planning of supervisory actions is based on a specific timetable for each insurance company, taking into account the results of quarterly reviews, regular or ad-hoc on-site inspections and additional information provided by companies.
In the framework of off-site supervision and monitoring actions, joint actions are also carried out, made up of specialists from the sectoral structure and specialists in preventing and combating money laundering from the independent structure of the FSA. In addition to the quantitative and qualitative analysis of all reports made under the legislation in force, the analysis of the policies underlying the governance system of insurance companies and the analysis of their strategy are carried out.

Surveillance measures (inspections and monitoring) of the insurance-reinsurance sector by type of entity and financial instrument (product) identified the following money laundering or terrorist financing threats between 2017 and 2020:

- Non-transparent clients of PEP (namely, with respect to the presentation of the source of funds used for insurance products with an investment component, unit link investment products/annuities);
- Non-resident clients accessing only insurance products with an investment component/unit link products/annuities;
- Non-resident customers in geographical areas identified as being included in the list of countries with deficiencies in the FATF standards;
- failure to appoint an Anti-Money Laundering Officer (AMLO – FATF R18) who meets all the conditions of competence and integrity necessary to manage threats and vulnerabilities in the business of high premium insurance or who belongs to a group established in other states.

Violations and deficiencies identified during inspections at the level of entities in the insurance sector (fundamental, thematic or ad hoc) are generally due to the following vulnerabilities:

- the lack or deficiencies identified in terms of preventive measures/control mechanisms (FATF R1, R18) implemented at the entity level;
- internal risk assessment (insurer, 2017)
- lack of training/training in the field of prevention and money laundering or financing of terrorism;
- deficient procedures regarding the knowledge of the clientele, the reporting of situations presenting risks of ML/TF, the additional measures of knowledge of the clientele for publicly exposed persons (1 insurer, 2018);
- non-compliance with the obligation to verify and document the beneficial owner (BOs) at the date of the claim related to investment accumulations or covered risk events;
- failure to report suspicious transactions to the FIU or reports containing poor quality information;
- limited access to information on beneficial owners, both nationally and internationally (1 insurer, 2017);
- Insufficient resources to cover money laundering or terrorist financing liabilities.

When assessing the appropriate and proportionate level of remedial measures and sanctions imposed on financial entities, the following shall be taken into account:

- The nature of the findings/deficiencies regarding the higher risk elements identified at the level of insurance entities and the insurance intermediation system/sector;
- The impact of the identified deficiency in terms of the entity's exposure to the non-banking financial sector/financial system;
- Use of available sanctions, including withdrawal of authorization/licence to operate;
- Publication of information on sanctions imposed on an entity to inform other entities in the sector so that they are aware of the measures needed to address similar risks.

From all these elements it was found that the insurance sector (for life insurance and unit link/annuities) presents an average risk and an average residual risk of being used for money laundering purposes from the assessment of identified ML/TF risks, vulnerabilities, threats and remedial measures and preventive response measures, in accordance with subchapter 6.3-6.4 point 4.2 of the NRA Methodology of the Council of Europe.

The type of products in the insurance sector that are subject to supervision for the purpose of preventing money laundering

Life insurance (AV)

In 2020, the contribution of life insurance companies to GDP was EUR 221 million. The share of life insurance activity in the total insurance sector in Romania from the perspective of the volume of gross premiums written is at a low level compared to other EU states.

Included in this insurance class are 7 subdivisions: C1 – life insurance, annuities and supplementary life insurance, C2 – marriage and birth insurance, C3 – life insurance and annuities, linked to investment funds, C4 – tontines, C5 – capitalization operations based on actuarial calculations, C6 – management of group pension funds and C7 – operations related to the duration of human life, in accordance with social insurance legislation.

In 2020, the volume of gross written premiums for the life insurance segment decreased slightly, while the value of written premiums for the general insurance business increased, which led to a decrease in the share of the life insurance sector to 19% of the total underwriting.

In the first 3 quarters of 2021, life insurance saw a 22% increase in the annual number of life insurance (taking into account all types of products on the market) maturing (paid to the insured/beneficiary) compared to the premiums 9 months of 2020, of which 25% for C1 – life insurance, annuities and supplementary life insurance and C3 – life insurance and annuities, related to investment funds. The gross written premiums related to life insurance (AV) are approximately RON 2 billion (approximately EUR 404 million[50]), which represents a significant increase of more than 22% compared to the first 9 months of 2020. Gross life insurance benefits are supplemented by maturity, partial surrenders and totals, all of which together amount to RON 622,066,730 (EUR 125.67 million), increasing by approximately 1.4% compared to the same period last year.

Figura 21 Evoluția volumului de indemnizații brute plătite, inclusiv maturități și răscumpărări pentru asigurări generale și de viață (miliarde lei)

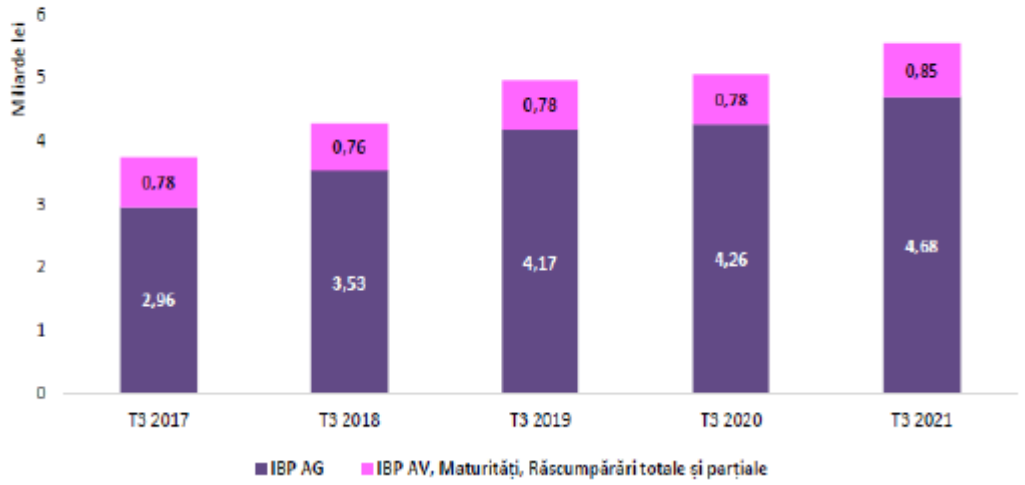


Table 14: dynamics of gross benefits paid, including maturities and redemptions for non-life and life insurance in the first 9 months of the period 2017-2021

Period	PBI AG + AV (lei)	Variation compared to period previous%	PBI AG (lei)	Variation compared to previous period%	GDP AV maturities, redemptions, total and partial (Lei)	Variation compared to period previous%
30.09.2017	3,734,894,025	—	2,957,268,881	—	777,625,144	—
30.09.2018	4,283,680,127	14.69%	3,526,518,510	19.25%	757,161,617	— 2.63%
30.09.2019	4,953,824,229	15.64%	4,169,900,048	18.24%	783,924,181	3.53%
30.09.2020	5,038,198,663	1.7%	4,258,607,436	2.13%	779,591,227	— 0.55%

[50] 1 EUR = 4.95 lei

30.09.2021	5,533,046,467	9.82%	4,682,758,309	9.96%	850,288,158	9.07%

The table - Dynamics of gross premiums written by insurance classes in the period 2016-2020

AV	C1	1.116.592.111	1.377.567.383	1.486.795.597	1.417.601.050	1.440.587.391
	C2	899.501	696.590	11.123	10.824	11.271
	C3	473.969.406	554.216.414	505.515.736	674.633.376	596.348.126
	C4	0	0	0	0	0
	C5	0	0	0	0	0
	C6	0	0	0	0	0
	C7	0	0	0	0	0
	A1	18.548.227	4.015.424	5.398.324	5.499.595	5.615.260
	A2	59.438.002	76.769.439	104.734.513	158.270.341	176.916.226
	TOTAL	1.669.447.247	2.013.265.250	2.102.455.293	2.256.015.186	2.219.478.274

A high concentration has also been maintained in the life insurance market, with 5 companies holding a share of about 81% of the total volume of premiums written in this segment, with cumulative underwriting exceeding RON 1.6 billion (EUR 323.23 million). Thus, we consider this to be a vulnerability of the Romanian insurance market due to the high degree of concentration, both in terms of exposure to the main classes of insurance supervised and in terms of the size of the market share held by a small number of insurance companies. Therefore, from a prevention and anti-money laundering perspective, this may lead to governance risks.

General vulnerabilities, considering life insurance products

In general, the money laundering risk associated with the life insurance sector is lower than that associated with other financial products (e.g. loans and payment services) or other sectors (e.g. banking, gambling, gemstones and metal dealers). At the moment, Romanian life insurance products are not flexible enough to be the first choice for money launderers. However, as with other financial services products, there is a risk that funds used to purchase life insurance are the proceeds of crime. There is also a potential risk that funds withdrawn from life insurance contracts could be used to finance terrorism.

ML/TF risks in the insurance sector can be found in life insurance and, at a lower risk compared to other life insurance products, in annuity-based products. Such products allow a policy holder to place funds in the financial system and possibly disguise their criminal origin or finance illegal activities.

At the same time, the sector review found that life insurance is not a product generally used by non-residents (low volumes). At the same time, in terms of customer monitoring, insurers report difficulties in obtaining information on PEP status.

Notably, money laundering or terrorist financing risks associated with life insurance products or product features that may be at risk of being used for money laundering or terrorist financing purposes (notwithstanding exposure to other money laundering or terrorist financing risk factors, such as transaction, distribution, geographic or customer risk) include:

(i) **Single premium insurance policies**: Policies that allow money launderers to offload large amounts of money in a single transaction (the most common form of money laundering for insurance companies). Money launderers will then try to get the money back through a fraudulent claim;

- Contracts of unit-linked type or single profit with premiums;
- Single premium cash value life insurance policies.

(ii) **Life annuity policies or the high value of premiums saved**: After paying premiums with proceeds of crime, money launderers can receive legitimate income from annuity policies or premium economy products.

(iii) **Cooling-off periods**: Money launderers may request refunds of premiums during a cooling-off period or may deliberately overpay premiums to trigger a refund;

- Endowment insurance;

(iv) **Surrendering the insurance policy**: Money launderers can surrender their policies at a loss to recover their deposited money;

- Indemnification or early termination of the insurance policy at any time, with reduced fees or charges;
- Accepting non-traceable payments such as cash, money orders, check cascades or virtual assets;
- Accepting frequent payments outside of a normal premium or payment schedule;
- Products that accept high value lump sums combined with liquidity features.

(v) **Supplements of funds**: After paying a small initial premium to avoid the attention of the authorities, money launderers can top up their payments to offload more criminal proceeds;

- Products that allow cancellation of a policy within a set time frame and refund of premiums paid;

(vi) **Transfer of ownership**: Customers can buy life insurance policies and transfer ownership to a criminal third party who later withdraws their money;

- Products that allow very high value or unlimited payments or large volumes of lower value payments;
- Products with features or services that allow customers to use the product in a manner inconsistent with its intended purpose (for example, an insurance policy designed to provide long-term investment opportunities but allowing frequent or low deposit/withdrawal fees);
- Products that allow assignment without the insurer being aware that the beneficiary of the contract has been changed until a claim is made;
- The customer is neither the payer nor the recipient of the funds;
- The source of payment or recipient of the funds is outside the jurisdiction (for example, the insurer in Jurisdiction A and the source of payment in Jurisdiction B); and

- Significant, unexpected or unexplained change in the customer's payment pattern, withdrawal or refund;

(vii) **Conditional loans**: After building up their value by paying premiums, money launderers can take out loans by securing them with their life insurance policy and using the cash value as collateral. Loans granted against policies do not involve strict anti-money laundering checks and do not have to be repaid: the loan amount and interest will be deducted from the death benefit;

- Products with features that allow loans to be taken out against the policy (especially where frequent loans can be taken out and/or repaid in cash);
- Agreeing to be used as collateral for a loan and/or issued in a discretionary or leveraged trust;
- Negotiability, for example, the product can be traded on a secondary market or used as collateral for a loan;

(viii) **GUARANTEES**: on single premiums can be used as collateral for bank loans, money launderers can surrender their policies for repayment of loans.
Vulnerability depends on factors such as (but not limited to) contract complexity and terms, distribution, payment method (eg cash or bank transfer) and contract law.

Health insurance

Health insurance continued to show a positive trend in the first 9 months of 2021, with an underwriting volume of about 384 million lei, increasing by more than 9% compared to the same period of the previous year and holding a 3.9% share of total gross premiums written by companies authorized and regulated by the FSA. The number of contracts in force at the end of September 2021 in the entire health insurance market is 356,296.

CASE STUDY:
An STR sent by Insurer A (branch of foreign financial entity) regarding the termination of two life insurance policies of Mr BB (individual, resident), identified as PEP and Rodna (August 2016).
The first life insurance, traditional type, started on 29.10.2005 until 29.10.2057, opened at the Dambovița county branch (where he lives), with a gross quarterly insurance value of 462,22 lei (approx. 102 EUR). The termination value of the contract was 8.198,48 lei (1.821 EUR).
The second life insurance policy was unit link M, with a gross quarterly insurance of 2,429.68 lei (EUR 539) started on 10/29/2005, with death beneficiary his wife. The value of the account at the time of the request to close the insurance was 37,687.12 lei (8,374 EUR) and the termination fee was 34,532.78 lei (7,673 EUR). In the application form for closure, the insurer laid down the rule that the payment should be made into a bank account (in this case, a bank account of the client).
In the insurance form, he stated that he was a director and administrator of his own company (it does not appear from public searches at the time of the execution of the insurance policy that he was a PEP). The insurer sent the STR before the transaction regarding the Rodna alert and the high amount of the early termination fee.
After analyzing the risk matrix of the item, the result is a medium risk of money laundering,

No.	Elements	Probability assessment	assessment consequences/impact	Risk level
1.	Risk	moderate	low	average
Associated vulnerabilities: **Lack of an internal alert system, lack of continuous monitoring**				
Associated threat: **Customers with criminal records;** **Publicly exposed persons associated with criminals;** **Designated person – international sanction**				
Event description: **The PEP client involved in criminal activities requested the early repayment of 2 life insurance policies, having a high value of the commission for the early termination of the contract;**				
Risk description: **Placement of possible illicit funds in life insurance products with possible early redemption action. Hence, using the life insurance product for the purpose of money laundering.**				

In 2020, health insurance accumulated gross written premiums in the amount of approximately 451 million lei, an increase of 18.38% compared to the same period of 2019:

- the gross written premiums (PBS) related to general insurance (GA) amount to 274 million lei, increasing by approximately 23% and representing approximately 61% of the total PBS for the health insurance activity;
- the gross written premiums related to life insurance (AV) amount to 177 million lei, increasing by approximately 12% compared to the similar period of the previous year.
-

The number of contracts in force at the end of December 2020 across the entire health insurance market stood at 377,854, down approximately 6% from the number of contracts in force at the end of 2019. The majority of contracts in force (350,668, representing approximately 93 % of the total number of contracts) are concluded for health insurance assimilated to general insurance.

All health insurance:

Period	Number of contracts in force at the end of the period of reporting (lei)	The number of us concluded contracts during reporting period	Gross premiums issued (lei)	Gross allowances paid (lei)
2016	231,198	271,836	172,819,942	68,373,126
2017	275,904	320,329	208,645,965	104,670,974

2018	365,872	427,290	335,020,775	164,564,666
2019	403,308	477,238	381,339,604	220,192,585
2020	377,854	486,485	451,445,204	213,095,277

Of which, these are related to life insurance contracts (AV):

Period	The number of contracts in force at the end	Number of concluded contracts in the	Premiums rough issued (lei)	Compensations paid rough (lei)
	reporting period (lei) of	the reporting period of		
2016	8,285	7,513	59,438,002	25,417,143
2017	10,144	3,710	76,769,439	32,179,374
2018	17,173	11,617	105.008.303	42,815,659
2019	36,596	26,219	158,270,341	73,205,852
2020	27,186	13,661	176,916,226	71,131,314

CASE STUDY:
STR (suspicious transaction report) carried out by the insurer AB regarding the gross underwritten payments of health insurance (594 lei, approx. 110 EUR) requested by an individual, GZ, in March 2016, who was identified at the time of payment as on the list of people affiliated with PEP with Rodna.
This situation demonstrates vulnerabilities such as: a faulty monitoring of the business relationship with this client of the insurer, which involved the application of the obligation to apply additional measures to know the clientele (EDD) and the faulty establishment of the risk category in which it should be included. Also, by accepting this client, the entity failed to comply with its own internal client acceptance policy and increased the entity's overall risk.
In this situation, FSA established a plan of measures, implemented by the insurer in 30 days.

No.	Elements	Probability assessment	assessment consequences/impact	Risk level
1.	Risk	low	moderate	average
Associated vulnerabilities: **Lack of an internal alert system, lack of continuous monitoring, lack of EDD**				
Associated threat: **Customers with criminal records;** **Politically exposed persons associated with criminals;** **possible group of people, clients associated with PEP investigated for financial crimes**				
Event description: **Affiliate PEP customer to investigate PEP using health events for unlocked money, very low premium level**				
Risk description: **Placing possible illicit funds in insurance and using the insurer for money laundering**				

Warranty insurance

Guarantee insurance registered a volume of gross written premiums of approximately 262 million lei in the first 9 months of 2021, down by 28% compared to the same life of the previous year (364 million lei). From the total gross premiums written by insurance companies authorized and regulated by the FSA in the first 9 months of 2021 (9.8 billion lei), the gross premiums written on the territory of other states recorded a volume of approximately 214 million lei, representing approximately 2. 2% of the total volume of

premiums subscribed, down compared to the same period last year (approximately 259 million lei).

Guarantee insurance is a form of insurance that provides full insurance for the execution of works, covering the risks arising from non-execution or improper execution of contractual obligations for any type of project, public and/or private, especially for those involved in the procedure, public procurement. The most used guarantees issued by insurance companies are:

- labor and warranty guarantees;
- performance guarantees (during construction, after construction);
- delivery guarantees;
- advance payment guarantees;
- payment guarantees;
- customs guarantees;
- various permit guarantees (eg environmental/land use guarantees).

In 2020, gross premiums written for guarantee insurance amounted to 465 million lei, registering an increase of over 68% compared to the same period of the previous year, respectively an increase of approximately 102% compared to the same period of 2018. as regards the value of the gross allowances paid, it was approximately 40 million lei, decreasing by approximately 3% compared to the same period of 2019.

Compared to the same period of the previous year, at the end of December 2020, the number of contracts in force in the insurance category increased by approximately 23%, reaching a number of 90,483 contracts.

This type of insurance can be vulnerable to fraud. These insurances have been used in the past to participate in public tenders.

Vulnerabilities to money laundering or terrorist financing risks of collateral insurance products or product characteristics that could be at risk of being used for money laundering or terrorist financing purposes (without prejudice to the exposure of other risk factors money laundering or terrorist financing risk, such as transaction risk, distribution risk, geographic risk or customer risk) include:

- Payment flexibility, for example the product allows unidentified third party payments or high value or unlimited premium payments, excess payments or large volumes of lower value premium payments or cash payments;
- Facilitating access to accumulated funds, for example the product allows partial withdrawals or early redemptions at any time, with limited fees or commissions;
- The possibility to easily change the beneficiary;
- Designing a product that allows a third party to deposit and make payments;
- the risk factor that triggers the payment of compensation cannot be determined objectively, the service provider (the insured person) can request at any time during the execution of the contracted service to use the insurance to cover the unexecuted part (for several reasons, including fraudulent).

ML/TF threats to this type of insurance are related to:

- the use of this type of collateral by criminals to use high-value transactions to integrate laundered money;
- using this type of guarantee from the criminal group formed by the person who controls the insurer, the executor of the work (the insured person) and the beneficiary of the insurance policy.

For this reason, this type of insurance may be vulnerable to fraud and may present a medium risk of money laundering.

Distribution channel

The share of income from insurance intermediation activity (insurance intermediaries) in the volume of intermediated premiums in the life insurance segment was 43.74% (the first 9 months of 2021), achieved by 169 insurance intermediaries. Therefore, in more than half of the cases, life insurance is underwritten directly by the insurer.

From the total gross premiums written by insurance companies authorized and regulated by the FSA in 2020 (11.5 billion lei), the gross premiums written on the territory of other states recorded a volume of approximately 355 million lei (78.88 million Euros[51]), representing approximately 3% from the total volume of premiums subscribed, increasing by approximately 38% compared to the previous year (approximately 257 million lei, 57.11 million Euros).

Period	Gross premiums issued (lei)			Intermediation of gross premiums (lei)			degree of Brokerage (%)	
	Total	AV	%	Total	AV	%	Total	AV
31.12.2016	9,380,935,173	1,669,447,247	17.80	6,200,117,078	170,709,691	2.75	66.09	10.23
31.12.2017	9,701,743,603	2,013,265,250	20.75	6,166,053,903	204,048,489	3.30	63.56	10.14
31.12.2018	10,144,526,431	2,102,455,293	20.72	6,380,788,060	237,540,165	3.72	62.90	11.30
31.12.2019	10,990,225,394	2,256,015,186	20.52	7,203,671,303	240,473,758	3.33	65.55	10.66
31.12.2020	11,500,479,256	2,219,478,274	19.29	7,859,221,295	287,079,947	3.65	68.34	12.93

In 2020, there were increases in brokered/distributed premium volumes for both types of life insurance classes, both traditional (class C1) and those with an investment component (class C3). As in previous years, life insurance with an investment component saw more pronounced growth in 2020 in terms of the volume of intermediated premiums.

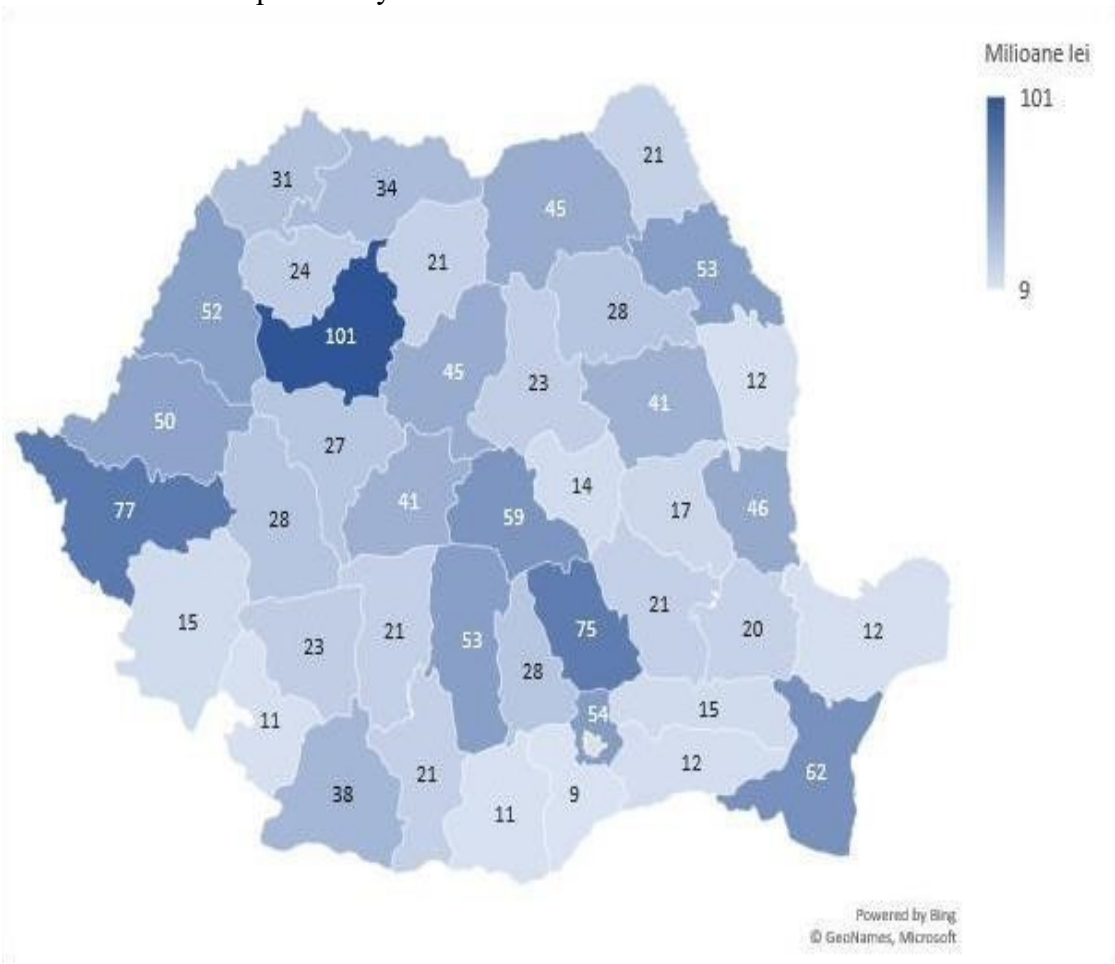
Class life insurance	The volume of intermediate premiums			Dynamics 2020/2019	Dynamics 2020/2018
	2018	2019	2020		
C1	199,110,236	206,423,054	232,827,926	12.79%	16.93%
3	21647.146	33,603,285	53,914,926	60.45%	149.06%

Geographic risk – vulnerabilities

Geographic distribution of life insurance (AV) is related to regional financial development (2020).

[51] 1 EUR = 4.5 lei

Regarding the geographical distribution of underwriting, it can be observed both in the case of general insurance (AG) and in the case of life insurance (AV), the most important cumulative value is the insurance contracts concluded in Bucharest and Ilfov, followed by the distance significant northwest, and the total value of the country insurance in the south is 9-101 million lei per county.



As a general risk, such a large difference in coverage with insurance products also means a very different use of them, with the most commonly used products being general insurance, especially vehicle insurance (RCA/ CASCO). From the perspective of the higher value of the compensations paid by the counties, they are related to the counties with the most insurances subscribed, with the exception of the PAD insurance[52]. Therefore, from this point of view, it may be a link between the number of insurance frauds/attempts and insurance coverage, e.g. in border counties where drivers prefer to subscribe in the neighboring country where car insurance is cheaper.

This creates an ML vulnerability to use the domestic insurance sector to cover claims caused by the insurance indemnity/direct compensation from the resident insurer in the event of a car accident. This risk cannot be linked to a fraud conviction, as it is not prohibited to take out insurance in another EU member state, but it can create a liquidity problem for the resident insurer and represents a money laundering vulnerability. ML vulnerabilities are related to:

[52]compulsory home insurance

- sales that are carried out without the presence of the customer (distance relationships), such as online sales, postal or telephone services, without screening measures appropriate, such as electronic signature identification or electronic identification documents;
- long chains of intermediaries;
- use of an intermediary in unusual situations (eg geographically unexplained distance);
- limited resources for ML obligations.

Money laundering threats are related to the ability of criminals to use the limited resources of brokers to use insurance products to place and integrate laundered money.

As for insurance intermediaries, when they conclude insurance products under the AML Law, they are reporting entities, which is why we consider them to be factors in mitigating the risks of money laundering. Intermediaries are well known by the insurer, who has ensured that the intermediary applies customer due diligence (CDD) commensurate with the risk associated with the business relationship[53].

Regarding insurance underwritten by branches of foreign intermediaries, as of December 31, 2020, 13 branches were operating in the insurance market, of which 10 were involved in general insurance (AG) and 3 were in life insurance (AV).

At the end of 2020, the branches accumulated gross written premiums amounting to 1.021 billion lei, up by approximately 15% compared to the previous year:

- gross written premiums (PBS) related to general insurance (AG) amount to 489.9 million lei, up by approximately 15% compared to the previous year;
- gross written premiums related to life insurance (AV) amount to 531.7 million lei, increasing by approximately 15% compared to the same period of the previous year;
- 12.69% of the health insurances were made through the branches.

Gross written premiums (lei) of branches	2018	2019	2020
AG	273,128,910	423,054,646	489,989,547
AV	396,241,305	464,278,869	531,761,035
TOTAL	669,370,215	887,333,515	1,021,750,583
AG (%)	40.80%	47.68%	47.96%
AV (%)	59.20%	52.32%	52.04%
Evolution of the volume of gross provisions paid, including maturities and redemptions			
AV	113,962,294	129,490,840	147,765,473
AV (%)	61.92%	51.43%	42.12%

Life insurance	Gross premiums written (lei)	Market share
A1, Accidents	349,686,867	65.76%
C1 – life insurance, annuity insurance and		29.12%

[53]PCT 14.14 of the EBA Risk Factor Guidance (revised 2021)

supplementary life insurance	154,870,354	
C3 – Life insurance and annuities related to investment funds	27,203,814	5.12%
Total	531,761,035	100%

In 2020, the branches reported gross indemnities paid, cumulatively for the two categories of insurance, in the amount of approximately 351 million lei, of which 148 million lei represent amounts paid for gross indemnities (including maturities and redemptions), related to life insurance, registering an increase of approximately 14% compared to the previous year.

Branches of financial institutions from Romania, within the FSA's AML supervision scope, are supervised by the FSA to ensure compliance with ML/TF obligations. No other threats and vulnerabilities have been identified for branches of non-bank financial entities in the EU, apart from those resulting from the previous analysis. This conclusion is the result of deficiencies found in controls and fit and proper assessments as well as supervisory assessments carried out together with the home country supervisor, as well as based on the insurance product offering and the type of clients.

4.4 Pawn shops, mutual aid houses, non-patrimonial entities and other non-banking financial institutions

Non-banking financial institutions (NBFIs), regulated by Law 93/2009 on non-banking financial institutions, are entities that carry out lending activity with a professional title under the conditions established by the legal provisions, the NBR being the only authority in a position to decide whether the activity carried out by an entity is of the nature of lending activity with professional title.

Non-bank financial institutions (NBFIs) that, in accordance with the legal provisions in force[54], have the quality of reporting entities supervised and controlled by NOPCML, are:
- *NBFIs* registered in the NBR's General Register, respectively pawnshops, mutual aid houses and non-patrimonial entities;
- *NBFIs* registered exclusively in the General Register of the NBR and which do not have the status of a payment institution or an institution issuing electronic money;

NBFI-registered in the General Register (NBR) can carry out the following lending activities[55]:
- **pawnshops**: granting loans with receipt of goods as pledge, respectively pawning through pawn shops;
- **mutual aid houses**: granting credits to the members of non-patrimonial associations organized on the basis of the free association consent of its members (employees/retirees), in order to support their members through financial loans by these entities;
- **entities without patrimonial purpose**: lending activities exclusively from public funds or made available on the basis of intergovernmental agreements;

[54]Art. 5 paragraph (1) letter b of Law 129/2019 with subsequent amendments and additions and art. 3 lit. a) from the Norms for the application of the provisions of Law 129/2019;
[55]Conf. art. 5 letter g and art 14 of (1) of Law 93/2009

NBFIs-registered exclusively in the General Register of the National Bank of Romania and which do not have the status of a payment institution or electronic currency issuing institution, can carry out the following lending activities: consumer loans, mortgage loans, real estate loans, microloans, transaction financing commercial, factoring operations, discounting, lump sum as well as financial leasing, issuing guarantees, assuming guarantee commitments, assuming financing commitments, other forms of credit financing.

During the reference period, supervision and control activities were carried out by the NOPCML for the NBR Registered NBFIs and for the NBR General Registered NBFIs that do not have the status of payment institution or electronic money institution, according to art. 10 letter b) of Law 656/2002, as follows:

1. During 2018 - 2019, a number of 2,386 NBFIs in the NBR's Register of Records, namely: 1490 pawnbrokers, 893 mutual aid houses and 3 non-profit entities[56]. By introducing them into an analytical process comprising a risk assessment matrix that reveals the degree of exposure to the risk of money laundering and terrorist financing of the reporting entity, based on a scoring system, the following results were obtained:
   a) In the case of pawnshops, from the 1,490 pawnshops supervised off-site 4.97% of the total were classified as high risk;
   b) In the case of mutual aid houses, of the 893 mutual aid houses supervised off-site, 8.2% of the total were classified as high risk;

2. In 2020, a total of 699 NBFIs were supervised off-site on a risk basis, as follows: 648 NBFIs: from the NBR's Register of Records, i.e. 508 pawnbrokers, 137 mutual aid societies and 3 non-profit entities, as well as 51 NBFIs from the NBR's General Register that do not have the status of payment institution or e-money institution. By introducing them into an analytical process comprising a risk assessment matrix that reveals the degree of exposure to the risk of money laundering and terrorist financing of the reporting entity, based on a scoring system, the following results were obtained:
   a) In the case of pawnshops, from the 508 pawnshops supervised off-site 8.1% of the total were classified as high risk;
   b) In the case of mutual aid houses, of the 137 mutual aid houses supervised off-site, 5.8% of the total were classified as high risk;
   c) For NBFIs from the General Register of the NBR *and which do not have the status of a payment institution or electronic currency issuing institution*, **of the 51 entities supervised off-site:** 53% of the total were classified as high risk;

3. During the reference period, a number of 103 NBFIs from the NBR's Record Register were supervised on-site (controlled), respectively: 60 pawn shops and 43 mutual aid houses. From the total of NBFIs in the NBR's General Register controlled, in more than half of them, i.e. in 51.4%, various non-compliance with the legal provisions in the field[57] were identified as a result, the control teams carried out training of the legal representatives of the audited entities on the best ways to comply with the relevant legal framework, with recommendations being recorded to remedy the infringements found and appropriate fines being imposed, where appropriate, as follows:

a) Out of the total number of pawnshops inspected, a total of 52 fines were imposed on 31 pawnshops for non-compliance with the obligations laid down in Law 656/2002.

[56] In accordance with national legislation - Law No 122/1996, Law No 540/2002 - mutual aid houses organized to support and provide financial assistance to associated members

[57] Law No 656/2002 republished

b) Out of the total number of mutual aid houses inspected, a total of 32 fines were imposed on 22 mutual aid houses for non-compliance with Law 656/2002.

General risks of the sector

In general, the sub-sector represented by NBFIs is lower risk as the customer base is almost entirely resident and the only products traded are (usually) loans.

However, the pawnshop sector, being a business that involves the frequent use of cash, is inherently risky as it can be exploited by criminals, representing a viable and simple option to hide the illegitimate proceeds of crime. Such cash-intensive businesses can enable the processing of large numbers of transactions that do not require the management of new technologies and tracking tools that can promote anonymity.

Mutual aid type NBFIs present a lower risk due to the nature of the products offered (loans granted to members of non-profit associations organized on the basis of the free consent of employees/pensioners), the source of funds being carefully assessed and, in principle, the only method of money laundering is early repayment from illicit sources.

General risks of the products/services offered in the sector

In the case of pawnshops, the value of transactions is usually low, which limits exposure to risk, as small loans are not as attractive to organized crime groups as other financial products, but can be used indirectly to launder criminal proceeds. Although transactions are usually small in value, criminals can spread large sums over several transactions. Therefore, the money laundering threat related to small value loans is considered moderately significant.

In the case of mutual aid houses (MAHs), due to the limited nature of the products, the fact that most entities have a resident customer base and offer small value loans, the risk is considered low.

Risk situations identified for the services provided/clients of the activity sector represented by NBFIs supervised by NOPCML:

- In the case of cash products/operations in which the customer:
  - Attempts to exchange low denomination notes for high denomination notes or numerous dirty, damaged or other suspicious notes.
  - He behaves atypically and requests that an unreasonably large amount of banknotes with a low nominal value be provided to him during the operation;
  - It requires the artificial splitting of some operations, for example to structure them below the reporting limit; carrying out in a short period several cash operations involving amounts below the reporting limit to NOPCML;
  - Sudden and unjustified increase in the frequency/value of operations performed by a customer;
- Substantial loans where collateral is redeemed well in advance of the due date and without a reasonable explanation as to the source of the funds used for repayment (such behavior, if repetitive, may attract greater suspicion);
- Making repayments using banknotes in denominations that are unusual for the pledge (ie repayment in large denominations);
- The customer provides confusing details about the loan or knows few details about its purpose;
- The customer provides false information or information that appears to be untrue;

- Suspicion that a customer is acting on behalf of a third party and is not disclosing that information;
- Customers attempting to use intermediaries to hide the true owner/beneficiary of traded goods or customers attempting to use a false identity;
- Customers who are reluctant to disclose information about the beneficial owner;
- Clients about whom reliable public sources indicate possible involvement in crimes generating illicit funds;
- Any situation where the knowledge measures applied highlight that the assets involved or the actual customers/beneficiaries come from high-risk geographic areas;
- Any situation where the knowledge measures applied highlight that the assets involved or the actual customers/beneficiaries come from high-risk geographic areas;

Overall vulnerability of the sector to money laundering risk and to specific products

The main vulnerabilities regarding the preventive measures identified in the supervision process at the level of financial institutions mainly arise from the finding of non-compliance with the legal provisions, with an emphasis on the following aspects:

- vulnerabilities regarding the ML/TF risk classification process for customers, the absence of risk assessment methodology and risk assessment or an inadequate product, transaction, distribution channel assessment process that resulted in customer awareness measures they were not applied by risk-based circumstantiation, not using the appropriate risk indicators for the risk-based assessment from the point of view of ML/TF;
- the measures to know the clientele applied do not in all situations allow the identification, as the case may be, of the real beneficiary of the customers
- lack or adequate procedures regarding the identification of publicly exposed persons;
- deficiencies regarding the reporting of all cash deposit/withdrawal operations from the cash register greater than the equivalent in lei of EUR 15,000 (in accordance with the provisions of art. 5 (7) of Law 656/2002 rep);
- insufficient measures regarding the training of employees regarding the provisions of the AML/CTF legislation and practical aspects that can facilitate their recognition of suspicious transactions (for example, the presentation of relevant case studies, the types of suspicious behavior, the legal and internal AML/CTF framework);
- the absence of procedures and control systems /inadequate procedures and control systems for identifying suspicious transactions;
- in the case of NBFIs, compliance systems and resources are not at the level of those available to credit institutions (banks), which resulted in the lack of an organizational AML/CTF risk culture;

Also, while the volume of transactions and the amounts at stake limit the sector's exposure to risk, the vulnerability is greater because managers of these businesses are less aware of ML/TF risks than the banking sector, and compliance systems and resources are not at the same level as the banks.

Conclusions – As a result of the supervisory and control activities, we consider that in particular pawnbroking NBFIs may be vulnerable to ML/TF risk due to deficiencies in the application of know-your-customer measures through risk-based circumstantiation and lack of awareness of the risks they may be exposed to from being used in illicit money laundering or terrorist financing activities.

"Fit and proper" mechanisms, registration/authorization and supervision mechanisms

According to the legal provisions[58], cannot hold the position of founder, shareholder, manager, administrator, member of the supervisory board, financial auditor of a non-banking financial institution:

- persons appoint in the lists[59] on preventing and combating terrorism;
- persons who, according to the law, are incapable or who have been convicted for crimes against the patrimony through breach of trust, embezzlement, misappropriation of funds, corruption crimes, abuse of office, taking or giving bribes, receiving undue benefits, influence peddling, money laundering, terrorism, forgery and use of forgery, tax evasion, perjury, crimes provided for by special legislation in the financial-banking field, by legislation on commercial companies, insolvency or consumer protection or for any other relevant facts;

Factors mitigating the risk related to pawnshops and NBFIs:

- The legal framework (they are reporting entities that cannot carry out activity without being registered in the NBR registers);
- The supervision and control of the way of applying the legislation in the field of AML/CTF is ensured by NOPCML, which periodically organizes training sessions dedicated to this sector;
- The existence of fit & proper mechanisms, respectively legal regulations in force that impose a series of conditions for founders, shareholders, managers, administrators, members of the supervisory board, financial auditors of non-banking financial institutions.

No.	Elements	Likelihood Rating (L)	Assessment of consequences (C)	Risk rating
	The risk of pawnshops and NBFIs	**Average**	**Moderate**	**Average**
Associated vulnerabilities: ***Pawn shops:*** **Frequent use of cash;** **Difficulties in identifying the real beneficiary of customers;** **Difficulties in determining the origin of funds/assets involved in transactions; NBFIs:** **Significant sums of money are transacted through NBFIs.** **Sector awareness of ML/TF risks still appears to be limited given the low level of reporting of suspicious transactions.**				
Associated threat: **The possible use by criminals, directly or through intermediaries, of the services related to this sector in order to conceal the illicit origin of some assets.**				
Description of the situation: **Money laundering through NBFIs could be possible by criminals or their intermediaries obtaining loans to repay using illicit funds, even if the associated costs are higher than other existing deals on the market, to benefit from the fact that the application of customer awareness measures can, in certain**				

[58] Article 16 of Law no. 93/2009 and Article 14 of Regulation no. 20/2009 regarding non-banking financial institutions

[59] Law no. 535/2004

cases, be less rigorous than in banks. The lack of due diligence by the entities in this sector regarding the prevention of money laundering/terrorist financing can be speculated by criminals or their interlocutors who, using the services offered by NBFIs, may try to place funds with an illicit origin by making related payments contracted loans.
Risk description: ***Medium risk*** ***Average probability*** ***Moderate consequences***

We consider that the exposure of the MAHs (mutual aid houses) to the risks of ML/TF is not significant because the "social fund" constituted by collecting sums of money from a large but known number of members is used for granting loans to MAH members, in the context where each of members (usually these are certain categories of pensioners, employees of various entities – an aspect that favors the optimization of the process of getting to know customers/the source of funds) can deposit only once a month an amount, as a rule reduced, according to the ceiling established by each MAH in part, and the value of the loans granted also cannot exceed certain limits established by the financial institution.

Regarding entities without patrimonial purpose, lending activities are carried out exclusively from public funds or made available on the basis of intergovernmental agreements. The use of the funds is carried out strictly for the purpose established following the agreements, and the amounts are of legal origin, therefore the exposure to ML/TF risks is low.

Factors that mitigate the risk related to MAHs and non-patrimonial entities:

- The legal framework (reporting entities that cannot carry out activity without being registered in the NBR registers);
- The supervision and control of the way of applying the legislation in the field of AML/CTF is ensured by NOPCML, which periodically organizes training sessions dedicated to this sector;
- The existence of fit & proper mechanisms, respectively legal regulations in force that impose a series of conditions for founders, shareholders, managers, administrators, members of the supervisory board, financial auditors of non-banking financial institutions;
- The amounts involved in the transactions do not usually have significant values, compared to other financial sectors, the MAHs practicing the application of ceilings for the loans granted, depending on specific criteria.

No.	Elements	Likelihood Rating (L)	Assessment of consequences (C)	Risk rating
	The risk of MAHs	**Average**	**Minor**	**Low**
Associated vulnerabilities: **Deficient application of some of the provisions of the legislation in the field of AML/CTF;**				
Associated threat: **MAHs are prohibited from lending to persons other than its members, cannot lend to legal entities, nor can they attract deposits or repayable funds.** **The funds of non-patrimonial entities are of legal origin, the use of the funds must be carried out in compliance with the purpose of the association/foundation.**				
Description of the situation: **MAH Associations (non-profit entities - legal entities that have the obligation to register according to the law) are organized based on the free consent of the members (employees/retirees, etc.), in order to support and help them financially by granting loans with interest that returns to the social fund of the members after deducting the statutory expenses.**				

Risk description:
Low risk ***Average probability*** ***Minor consequences***

4.5 Currency exchange offices

General description

In Romania, currency exchange offices are authorized by the Ministry of Finance - through the Commission for the authorization of currency exchange activity, according to the rules of the Order of the Minister of Public Finance no. 664/2012 of May 14th, 2012 regarding the authorization and/or registration of entities carrying out currency exchange activities on the territory of Romania, other than those subject to the supervision of the NBR.

The Commission may order the cancellation of the foreign exchange authorization issued to an entity and of all statistical codes allocated to it where it is established that, at the time of granting the authorization, the applicants have provided incorrect or inaccurate information which, if known, would have led to the authorization or statistical codes not being granted. In addition, the Commission may order revocation or cancellation, as appropriate, at the request of the NOPCML, for non-compliance with the provisions of the legislation on money laundering and terrorist financing[60].

In Romania, the foreign exchange market includes the following segments:

- the interbank currency market on which currency transactions are carried out by credit institutions, as well as by the NBR, in accordance with the regulations issued in this regard by the NBR;
- the foreign exchange market of entities authorized to carry out foreign exchange activities.[61]

Entities authorized to carry out foreign exchange activities (being prohibited from carrying out foreign exchange activities by entities other than these) include:

- entities that carry out currency exchange activity in the banking system, based on express legal provisions and have stipulated currency exchange activities in the constitutive acts that regulate their establishment and operation.
- entities authorized to carry out currency exchange activity for natural persons, respectively:

  - currency exchange houses, organized as legal entities according to Law no. 31/1990 on companies, having as its main object of activity the activities of

[60] Order no. 664/2012 of May 14, 2012 regarding the authorization and/or registration of entities that carry out foreign exchange activities on the territory of Romania, other than those subject to the supervision of the NBR

[61] Regulation no. 7 of August 4, 2020 for the amendment and completion of NBR Regulation no. 4/2005 regarding the currency exchange regime

currency exchange for natural persons CAEN code 6612 - Intermediation activities of financial transactions - activities of currency exchange offices;
- the entities that manage tourist reception structures with tourist accommodation functions and have as their object of activity currency purchase operations (quoted and unquoted) in the form of cash and cash substitutes;

Currency exchange offices are supervised, with regard to the way of applying the provisions of Law 129/2019, by NOPCML.

According to the website of the Ministry of Finance, on December 1st, 2021, on the territory of Romania there were 458 entities authorized to carry out foreign exchange activities and 2677 foreign exchange points, other than those that are subject to the supervision of the National Bank of Romania.

The analysis of the cases investigated by the law enforcement authorities indicated that, during the reference period, foreign exchange operations constituted a channel used for money laundering in a case where a conviction was ordered.

Results of surveillance activity

During the reference period, NOPCML carried out surveillance activities for currency exchange offices, a number of 198 currency exchange offices were supervised off-site, following the analysis and processing of related data and information, 27.7% of the entities being included at a high degree of risk.

During the same reference period, the NOPCML supervised on-site a total of 72 foreign exchange offices, as a result of which a number of breaches of the legal provisions in the field of AML/CTF were identified. As a result, the control teams have trained the legal representatives of the entities checked on the best ways to comply with the legal framework in this area, and appropriate fines have been imposed and recommendations have been recorded to remedy the violations found.

Foreign exchange service providers - currency exchange houses - tend not to always have the capacity, experience and resources to effectively implement AML/CTF requirements.

The NOPCML, as supervisory authority, has an important role to play in providing appropriate guidance to foreign exchange offices. In this regard, in addition to the trainings carried out during the verification and control actions, the NOPCML organized during the reference period, together with the MF, three trainings that focused on this sector of activity, addressing practical aspects on the application of legal provisions in the field of AML/CTF, types of ML/TF, implementation of the international sanctions regime. In addition, a series of manuals and guides developed by the NOPCML for the guidance of supervised entities are published on the www.onpcsb.ro website in the Guides section.

Conclusions – From the questionnaires processed (used in this assessment) and the supervisory work, it appeared that the entities concerned - the foreign exchange offices - are in many cases aware of and apply anti-money laundering and anti-terrorist financing legislation, but there is a need to raise awareness within this sector, as in several compliance checks it was found that employees of the entities in this sector were not properly applying customer identification and KYC measures.

Vulnerability of internal control mechanisms, highlighted following the supervision activities carried out by NOPCML:

- lack of effective monitoring systems based on which entities can consistently identify money laundering/terrorist financing risks;
- the insufficiency of human and material resources allocated by the entities to the activity of preventing and combating ML/TF;
- the verification and control actions carried out by NOPCML highlighted the fact that the degree of awareness in this sector is however uneven.

According to the analyzes carried out by the authorities, in terms of exposure to the risk of ML, currency exchange houses were assessed as a vulnerable sector.

Although the extent of the phenomenon is difficult to assess, the analysis indicates that organized crime groups can use foreign exchange to launder the proceeds of crime, which leads to an increase in the level of vulnerability. Awareness in this sector is not uniform, leading to increased exposure to ML.

At the same time, within the Supranational Risk Assessment[62] it was mentioned that terrorist groups have a certain tendency to use foreign exchange to support/carry out their operations, and this boarding does not require any specific planning or experience, these aspects leading to an increase in the sector's exposure to TF.

According to one of the FATF guidelines,[63] several case studies have shown that foreign exchange transactions have been used both in money laundering activities at all three stages of the process (placement, layering and integration) and (in some cases) for terrorist financing purposes. The ML/TF exposure risks related to the foreign exchange sector may be predominantly in relation to real customers/beneficiaries. Case studies have also highlighted links within this sector between money laundering and other criminal activities (e.g. fraud, human trafficking, smuggling, drug trafficking, economic crime). It has also been noted that, being often smaller businesses, foreign exchange operators can be co-opted by criminals and used in the money laundering process, so the role of smaller entities within the sector should not be underestimated.

General risks of the products/services offered in the sector

The currency exchange sector is prone to the risk of ML/TF as the nature of the products offered (cash transactions, many private clients, numerous and often low-value transactions, etc.) creates the context that sometimes the employees/representatives of the entities not to perform all the necessary diligence in situations that require:

- applying the appropriate measures to identify the source of the funds used in the currency exchange operation;
- adopting appropriate measures to know the clientele/real beneficiaries, within a risk-based approach;

[62] SNR

[63] https://www.fatfgafi.org/media/fatf/ML%20through%20Remittance%20and%20Currency%20Exchange%20Providers.pdf (Money Laundering through Money Remittance and Currency Exchange Providers)

- reporting to the NOPCML operations that present indications leading to the suspicion of money laundering/terrorist financing;
- the use of the tools and mechanisms of the internal control system in order to identify the risks of money laundering;
- allocating sufficient resources to the departments responsible for compliance activity in the field of preventing and combating money laundering and terrorist financing;
- checking clients on publicly exposed persons lists and/or international sanctions lists;
- identification and verification of clients and real beneficiaries of transactions;
- adequate monitoring of transactions, requesting identity documents when carrying out transactions, keeping identity references within the term provided by law and requesting a declaration of the origin of the money source;
- assigning clients to the corresponding risk category and applying, as appropriate, additional measures to know the clientele;
- superficially treating or completely ignoring aspects/situations that could lead to suspicions of money laundering (for example, repeated requests to a foreign exchange office for currency purchase/sale transactions in amounts immediately below the reporting ceiling, situations where : the customer frequently asks for currency in high-value banknotes, the customer has suspicious/atypical behavior, the customer does not seem to be interested in the exchange rate, shows up at the counter of the currency exchange office with very large amounts of cash, situations where the same customer frequently performs multiple cash exchange operations in various currencies using units from several work points, requests to exchange large amounts of "slow" currency - not used frequently).

Overall vulnerability of specific sector/products to money laundering risk

According to SNRA[64], in the case of currency exchange houses, compliance checks should include checks on the fulfillment of the obligation to ensure training of employees on the recognition of suspicious transactions and legislation in the reference area.

Clearly, AML/CTF through foreign exchange activity raises a number of regulatory and especially enforcement challenges, with low detection of money laundering compared to the size of the industry as a whole. Vulnerabilities related to the sector are enhanced not only by the fact that criminals with illicit funds can easily use this type of operations (without having to resort to specialist advice), but also by the deficiencies that certain entities in the sector have with regard to complying with some obligations arising from the legislation in the field of preventing and combating ML/TF, the lack of diligence can be speculated by those who intend to identify opportunities to hide the origin of some assets.

Currency exchanges can be an important link in the money laundering chain, especially at the placement stage. Once the money has been exchanged into another currency, it becomes more difficult to trace its origin. In addition, due to the occasional nature of transactions, representatives of foreign exchange houses find it particularly difficult to carry out continuous monitoring to detect anomalies and risk profiles.

Fit&proper mechanisms, registration/authorization and supervision mechanisms

[64]REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the assessment of money laundering and terrorist financing risks affecting the internal market and linked to cross-border activities - Brussels, 24/07/2019

In Romania, currency exchange houses have a legal framework both for authorization/operation and for the prevention and combating of money laundering and the financing of terrorism.
Entities intending to carry out foreign exchange activities must obtain authorization before starting the activity from the Foreign Exchange Activity Authorization Commission, meaning that they must cumulatively meet a series of conditions imposed by the legal framework[65] (including: evidence of the approval of law enforcement authorities granted to all directors, significant shareholders or associates holding at least the same percentage of shares as required for a significant shareholder, and the entity has not been convicted by a final judgment of conviction for which no rehabilitation has occurred), which is a factor mitigating the risk to which this sector is exposed.

Conclusions:

During the compliance checks carried out by NOPCML, situations were identified several times in which the application of customer due diligence measures was carried out incorrectly, situations in which cash transactions were not reported, situations indicating the lack of adequate internal controls regarding the concrete way of applying the provisions of the rules/procedures approved by the management within the carried-out activity.

Risk mitigating factors:

Customers are natural persons who, as a rule, carry out operations with relatively small amounts.

The supervision and control of the way of applying the legislation in the field of AML/CTF by this category of reporting entities is ensured by NOPCML, which periodically organizes training sessions dedicated to this sector;

Existence of fit&proper mechanisms – for authorization/operation.

The degree of awareness regarding the obligations deriving from the legislation in the field of preventing and combating money laundering/terrorist financing is satisfactory in this sector, since between 2018 and 2020 NOPCML received a number of 146 reports of suspicious transactions from entities that carry out foreign exchange activities.

No.	Elements	Likelihood Rating (L)	Assessment of consequences (C)	Risk rating
	The risk of currency exchange houses	Average	Moderate	Average
Associated vulnerabilities: **Intensive use of cash;** **The large number of customers to whom simplified measures of knowledge apply.**				
Associated threat: **Poor application of knowledge measures;**				
Event description: **Amounts from criminal sources can be subjected to successive currency exchanges, in various currencies, to facilitate complex operations aimed at disguising the real origin of the assets involved.**				
Risk description: ***Medium risk***				

[65] OMFP 664/2012

Average probability ***The consequences are moderate***

4.6 Postal service providers providing payment services

According to national legislation, postal service providers providing payment services are financial institutions[66].

A postal service provider can be any authorized natural person, sole proprietorship, family enterprise or any legal entity whose activity consists, always in part, in the provision of one or more postal services[67].

The general authorization regime is the legal regime[68] adopted by the National Authority for Administration and Regulation in Communications (hereinafter referred to as ANCOM), which establishes the rights and obligations of postal service providers, allowing the provision of postal services without obtaining an explicit decision from ANCOM, by notifying the intention to provide postal service provision activities. Notification is considered made only if all legal requirements regarding the transmission, form and content of the notification have been fulfilled. Until the notification has been made, the applicant is not entitled to provide postal services.

According to the law on payment services[69], several categories of entities can provide payment services on the territory of Romania, including giro postal service providers that provide payment services according to the applicable national legislative framework.

The NBR is the responsible competent authority[70] with the assurance and monitoring of compliance with certain provisions of the Law on Payment Services, of the regulations issued in application of those legal provisions as well as of the delegated acts adopted by the European Commission in the field of payment services, by several categories of entities, including suppliers of giro postal services that provide payment services.

National legislation stipulates the obligation of payment service providers[71] to establish a framework of mitigation measures and adequate control mechanisms to manage operational and security risks, related to the payment services they offer. At the same time, along with other categories of entities, giro postal service providers that provide payment services have the obligation[72] to provide the National Bank of Romania annually, in the form requested by it, an updated and complete assessment regarding the operational and security risks related to

[66] Article 2 letter (g) point 1 of Law no. 129/2019 for preventing and combating money laundering and terrorist financing

[67] Art. 2 point 2 of GEO no. 13/2013 on postal services

[68] Decision of the President of the National Authority for Administration and Regulation in Communications No 313/2017 on the general authorisation regime for the provision of postal services

[69]Decision of the President of the National Authority for Administration and Regulation in Communications No 313/2017 on the general authorisation regime for the provision of postal services

Article 2 letter from LAW no. 209 / 2019 regarding payment services and for the modification of some normative acts

[70]Article 223 paragraph (1) of LAW no. 209 / 2019 regarding payment services and for the modification of some normative acts

[71]Article 218 paragraph (1) of LAW no. 209 / 2019 regarding payment services and for the modification of some normative acts

[72]Article 218 paragraph (2) of LAW no. 209 / 2019 regarding payment services and for the modification of some normative acts

the payment services they offer, regarding the degree of adequacy of the mitigation measures and the control mechanisms put in place in place in response to these risks.

Also, according to the legal provisions[73], payment service providers - Romanian legal entities, which provide payment services on the territory of Romania, as well as on the territory of other member states through branches, agents or directly, have the obligation to notify the National Bank of Romania of any operational incident or major security, without unjustified delays and in the form requested by the NBR. The mentioned entities also have the obligation[74] to provide the NBR, at least annually, with statistical data on fraud related to different means of payment.

From the analyzes carried out by the law enforcement authorities, it emerged that the postal services were mentioned in only one conviction, only in the sense that connections with that sector existed in connection with the laundering of sums of money obtained from bribes.

According to NOPCML statistics, in the period 2018-2020 postal service providers did not submit STRs, therefore this aspect could indicate a low level of information in this sector regarding the fight against money laundering and terrorist financing.

During the reference period, surveillance and control activities were carried out for commercial companies - authorized postal service providers (selected from the list of providers available on the ANCOM website) as follows:

A number of 12 entities were supervised off-site, on a risk basis; following the analysis and processing of related data and information, based on a scoring system, approximately 50% of the entities were classified as high risk.

During the reference period, a number of 4 entities - postal service providers - were supervised on-site; non-compliances were identified in all 4 entities that required the formulation of specific recommendations in the control document.

Penalties were also imposed for non-compliance with legal provisions concerning: application of know-your-customer measures, designation of one or more persons with law enforcement responsibilities/obligation to establish appropriate policies and procedures, how to implement international sanctions.

General risks of the sector

The sector can be used by people who have significant amounts of money from crimes, sums which they subject to a process of division, using a complex circuit of transfers, involving a large number of interlocutors from various geographical areas, often located as far as possible away from the area where the predicate crime was committed, the purpose being to make it more difficult to trace illicit funds.

General risks of the products/services offered in the sector

[73]Article 219 paragraph (1) of LAW no. 209 / 2019 regarding payment services and for the modification of some normative acts

[74]Article 219 paragraph (6) of LAW no. 209 / 2019 regarding payment services and for the modification of some normative acts

Significant amounts can be transferred by using such services, by dividing them into smaller amounts, below the reporting limit to NOPCML, the purpose being that the operations are not detected, no additional measures are applied.
Being intended for the general public, the use of these services does not involve significant costs and can be easily accessible to criminals, with no prior specialization/experience required.

The overall vulnerability of the sector/specific products (services) to the risk of money laundering

Vulnerabilities regarding the preventive measures identified within the sector surveillance activities mainly arise from the finding of deficiencies regarding the application/adoption of specific measures, for example insufficient measures in relation to:

- the distinct highlighting within the internal procedures of the risks specific to each product/service;
- the application of measures to know the clientele / real beneficiaries / regarding the way of implementation of international sanctions;
- the identification and inclusion in internal procedures of specific indicators for recognizing suspicious transactions;
- appropriate training of employees regarding the provisions of the legislation in the field of preventing and combating money laundering / terrorist financing and practical aspects that can facilitate their recognition of suspicious transactions.

Fit and proper mechanisms, registration/authorization and surveillance mechanisms

NOPCML supervises and controls postal service providers authorized by ANCOM that provide payment services, regarding how to apply the provisions of the law to prevent and combat money laundering and terrorist financing[75]. We also mention the fact that in the application of Regulation (EU) 2015/847 NOPCML is designated as the authority responsible for the supervision and control of compliance with the provisions regarding the information accompanying the transfers of funds - for postal service providers that provide payment services according to the applicable national legislative framework[76].

Risk mitigating factors in the sector.

According to the law on payment services, payment services can be provided by giro postal service providers on Romanian territory, and the NBR is the competent authority responsible for ensuring and monitoring compliance with some provisions of the Law on payment services. Postal giro service providers that provide payment services are obliged to provide the National Bank of Romania annually with an updated and complete assessment of the operational and security risks related to the payment services they offer, regarding the adequacy of mitigation measures and the control mechanisms implemented in response to these risks.

NOPCML supervises and controls postal service providers authorized by ANCOM that provide payment services, regarding how to apply the provisions of the law for the prevention and combating of money laundering and terrorist financing and periodically organizes

[75]According to art 3 letter a) of the Norms for the application of the provisions of Law no. 129/2019 approved by Order of the ONPCSB President no. 37/2021
[76]Art. 29 paragraph (1) letter b of Law 129/2019

training sessions, in which theoretical and practical aspects are presented intended to facilitate in-depth knowledge of relevant aspects in the reference field and awareness of risks.

No.	Elements	Likelihood Rating (L)	Assessment of consequences (C)	Risk rating
	Risk of postal service providers providing payment services (giro)	**Low**	**minor**	**Low**
Associated vulnerabilities:				
Low costs; **The reporting entities' low awareness of the risks of exposure of the sector to ML/TF.**				
Associated threat: **failure corresponding to, on the base of risk, of measure of knowledge of the clientele/beneficiaries and the lack of indicators to recognize suspicious transactions specific to the sector may constitute opportunities for persons intending to launder money.**				
Event description: **By using the services offered within the sector, multiple transfers are possible (fractionation into smaller amounts, below the reporting limit to NOPCML), so that operations involving funds of possible illicit origin cannot be easily detected.**				
Risk description: ***It is low risk*** ***Low probability*** ***The consequences are minor***				

4.7 DNFBPs

4.7.1 Games of chance service providers

General description

In Romania, the organization and operation of games of chance is authorized by the National Office for Games of Chance (hereinafter referred to as ONJN) - responsible for authorizing, controlling and monitoring gambling, the sector being regulated by specific legislation[77].

The ONJN, an institution responsible for the regulation, sectoral supervision and control of the games of chance market, subordinate to the Ministry of Finance, was established for the purpose of unitary management of some databases and an IT system for monitoring and control in the field, which would allow the reduction tax evasion, the adaptation of gambling regulations to the dynamics of this extremely active field, the need to ensure the prevention of gambling addiction and the fight against the illegal sector of gambling by strengthening the technical and legal instruments that allow the detection and sanctioning of illegal operators[78].

The organization and exploitation of games of chance is carried out by the persons who hold the license to organize and the authorization to exploit games of chance, issued by ONJN, which can grant an organization license and exploitation authorization for the following gambling activities:

[77] GD no. 111/2016 for the approval of the Methodological Norms for the implementation of the Government Emergency Ordinance no. 77/2009 regarding the organization and exploitation of games of chance and for the amendment and completion of Government Decision no. 298/2013 regarding the organization and operation of the National Office for Games of Chance, amended and supplemented by HG no. 644/28.08.2013.

[78] ONJN website: http://onjn.gov.ro

a) **traditional games of chance (offline**): lotto, betting (mutual betting, fixed-odds betting or counterparty betting), casinos, poker, slot machine activities, bingo activities conducted in gambling halls, bingo activities organized through television network systems, activities of temporary games of chance (organized in tourist resorts or aboard cruise ships), raffle games;
b) **remote games of chance (online**): lotto, remote casino gambling activities including slot games, betting (remote fixed odds betting, remote mutual betting, remote counterpart betting) remote bingo and keno games, remote raffle luck.

According to the ONJN's Activity Report, in 2020, a total of 360 gambling organizers carried out activity (a decrease compared to 2019 when 369 gambling organizers carried out activity and compared to 2018 when carried out activity 387 organizers of games of chance) and a number of 411 economic operators licensed second class, as follows:

a) 30 gambling organizers fixed odds bets;
b) 1 mutual betting gambling organizer;
c) 1 lotto gambling organizer;
d) 7 organizers of games of chance characteristic of the activity of poker clubs;
e) 4 organizers of games of chance characteristic of casino activity;
f) 6 organizers of bingo games of chance held in gaming rooms;
g) 1 organizer of games of chance characteristic of the poker festival activity;
h) 285 organizers of slot-machine gambling games;
i) 25 remote gambling organizers;
j) 411 economic operators holding a class II license (companies that have the right to promote online gambling activities, software providers and other services relevant to gambling).

In 2020, NOPCML received a total of 40 STRs from entities in the games of chance sector. Also, between 2018 and 2020, 10 cases were identified in the games of chance sector, which were based on STRs sent by the banking system.

In the above-mentioned cases, indications of money laundering of the proceeds of predicate offences committed in the territory of another state (i.e. tax evasion, trafficking in human beings/pimping and phishing and skimming) have been identified. Resident and non-resident legal entities and resident individuals were involved in these offences, the recycling of illegal funds taking place under the cover of gambling in casinos, bookmakers and online betting platforms. Thus, money illegally obtained by organized criminal groups from other countries was transferred to Romania to be introduced into the legal circuit by placing it in the gambling system through the use of gambling activities. The operational mechanisms used in this case involved the involvement in the financial circuits of operations carried out by exponents of networks active on the national territory through casinos, betting operators and specialized online betting platforms.

General supervisory framework

During the analyzed period, the legislative framework that regulated the activity of supervision and control in the field of games of chance was modified as follows: until 2019, only casinos were subject to the law, and the verification and control of the way of applying the provisions of the law belonged to NOPCML, and starting on July 11th, 2019, through the adoption of Law 129/2019, all "games of chance service providers" are considered reporting

entities[79], the manner of application of the provisions of the law being supervised and controlled[80] on the one hand by NOPCML and on the other hand by ONJN.

During 2018, NOPCML supervised off-site casino gambling operators[81] by introducing them within an analytical process that includes a risk assessment matrix that reveals the degree of exposure to the risk of money laundering and terrorist financing of the reporting entity. The entities assessed at the highest degree of risk were included in the Program of on-site verification and control actions and verification and control actions were started at the entities' headquarters.

As a result of the on-site control actions carried out at 4 casinos, a number of violations of the legal provisions in the field of AML/CTF were identified, as a result, the control teams carried out the training of the legal representatives of the audited entities on the best ways to comply with the legal framework in this matter, and the appropriate contravention penalties were applied and at the same time a number of recommendations were recorded for the audited entities to remedy the violations found.

In conclusion, vulnerabilities of the sector highlighted from the analysis of the results of the surveillance activities mainly reside in the finding of non-compliance with the legal provisions, with an emphasis on the following aspects:

- in several situations the applied KYC (know your customer) measures did not allow the identification of the real beneficiary of the customers;
- KYC measures were not applied through risk-based circumstantiation, as the appropriate risk indicators were not used for the risk-based assessment from the ML/TF point of view;
- deficiencies regarding the reporting of all cash deposit/withdrawal operations from the cash register greater than the equivalent in lei of EUR 15,000;
- insufficient measures regarding the appropriate training of employees regarding the provisions of the legislation in the field of AML/CTF and practical aspects that can facilitate their recognition of suspicious transactions (for example, the presentation of relevant case studies);
- deficiencies regarding the establishment/completion/updating/reassessment within the internal procedures of anomaly indicators for the recognition of suspicious transactions.

NOPCML organized a series of training sessions for gambling service providers, the subject of the training aimed at practical aspects regarding the application of legal provisions in the field of AML/CTF, types of ML/TF, implementation of the international sanctions regime.

The main AML compliance issue identified for casinos is that their money laundering risk assessment, policies, procedures and controls, including customer risk profiling, customer due diligence and ongoing monitoring, has become more of a formal exercise of ticking boxes, without paying due attention to the importance of taking a risk-based approach and how this affects their ability to implement fit-for-purpose policies, procedures and controls, as well as effective employee training.

[79] According to art. 5 para. (1) lit. d) from Law 129/2019
[80] According to art. 26 - (1) of Law 129/2019
[81] Provided for in art. 10 lit. d) from Law 656/2002

Regarding the regulatory activity, by order no. 370/2021, published in MO no. 21/07.01.2022, ONJN adopted, "Instructions on the prevention and combating of money laundering and the financing of terrorism in the field of games of chance" by which a series of measures were established to prevent and combat money laundering and the financing of terrorism through the activities carried out by gambling service providers, measures that will have a dissuasive effect on persons interested in money laundering or terrorist financing through gambling.

At the same time, ONJN, as the anti-money laundering and anti-terrorist financing supervisory authority for casinos and gambling service providers, has the power to impose sanctions for AML/CTF violations.

From the questionnaires processed, according to the procedure for carrying out the national risk assessment, it emerged that most of the entities in the gambling sector, which were part of the sample analyzed, indicate that they have an elusive general knowledge in the field of combating money laundering and terrorist financing, and do not have a thorough knowledge of the legislation that applies in this area.

General risks of the sector

In relation to gambling, the risk of infiltration or possession by OCGs (organized crime groups) was highlighted. Thus, casinos are attractive to organized crime, in the sense that certain criminal groups take control of them, giving them the opportunity to launder their illicit proceeds, but also to engage in other types of crime. In this case, we mention the use of this technique by individuals - recognized members of OCGs - who, in the process of placing and layering illegally obtained funds, transfer the cash amounts to different countries where gambling is authorized, other than the countries of origin where they operate illegally, as a destination for money laundering. However, the national licensing system through the conditions imposed (detailed below) by the ONJN so that the regulator ensures that the legal representatives/partners/managers/real beneficiaries of the entities in the sector are suitable and competent persons who can protect those entities against their misuse for criminal purposes, diminishes the ability of the OCG to infiltrate the ownership/control of gambling activities.

Casinos and other gambling entities are vulnerable to being used by money launderers because they offer the possibility of intensive use of cash. At the same time, in the case of traditional gambling, there may be a risk of attempting to bribe, influence or corrupt a casino employee in order to avoid suspicious transaction reporting obligations. In Romania, casinos do not provide their customers with proof of winnings or losses, and this may also be in the interest of criminals, as they can claim that the funds at their disposal come from legal winnings. As both the payment methods accepted and the speed at which financial transfers are made increase, so does the ability to mask the source of funds where methods offer greater anonymity.

In the case of online gambling, the exposure to money laundering risk is high because it includes significant factors such as: lack of physical presence of players, significant and complex volumes of transactions and financial flows. Although not cash-based, the sector is closely linked to the use of electronic means of payment and virtual currencies, which increases the degree of anonymity for customers, with virtual currencies being attractive for cybercriminals to use. Although the gambling sector continues to make improvements in terms of preventing and combating money laundering and terrorist financing (mainly through

staff development efforts), it is noted that these efforts are not yet comprehensive enough to reduce anti-money laundering risks and there are still specific training gaps for staff in the sector.

General risks of the products/services offered in the sector by gambling category

A. CASINOS

As regards casinos, the legislation provides for strict systems to prevent fraud, to protect against any criminal activity and to regulate the fight against money laundering and the financing of terrorism. However, casinos can still be exploited as a channel for money laundering, with a number of risks identified such as:

- the high volume of cash transactions (although the sector has also developed alternative means of payment);
- carrying out usury activities on the premises of the gambling organizer;
- concealing the identity of the real beneficiaries (for example, when the ID card is checked when the customer enters the casino but not when he buys chips);
- crediting players;
- the presence of "High roller" customers, who break up the staked amounts into small stakes, so as not to become suspicious;
- losing considerable amounts at the gaming table, in favor of certain players, or a certain person, when the games offered are not organized "against the house";
- disguised purchase of chips (with cash or electronic means of payment), where the person may try to hide illicit income by disguising it as casino winnings (e.g. by buying chips but not using them for gambling, including to other players, so that the funds represent legitimate winnings);
- game rules can potentiate the risk of money laundering (for example, if a game allows customers to place bets on each side of the betting event (baccarat, craps or roulette), affiliated players could bet on both sides in order to launder game funds;
- in the case of poker, a game that is not played "against the house", there may be suspicious transactions between customers at the gaming tables;
- participation in the game through intermediaries;
- providing customers with currency exchange services, player deposits and other financial services;
- players residing abroad, including in particular players from countries that are not part of the EU / EEA or are not included in the FATF list;
- minimal nature of the actions of the person designated with responsibilities in the field of AML/CTF, through the formal application of the legal obligations imposed on him by law;
- players reluctant to provide information;
- casual players, including tourists who may be at increased risk given their deviation from normal behavior;
- complicity of employees in carrying out illegal actions.

During the Focus Group discussions held as part of the risk assessment process, representatives of the casino sector expressed their concern about the application of know-your-customer measures with a limited period of time available. Applying know-your-customer/beneficiary measures has been identified as a major challenge, particularly for online gambling. The online gambling sector's use of stolen and forged identities has been identified as a specific threat.

B. BETTING

In terms of betting, the risks could include:

- presence of cash transactions;
- the anonymity of customers, who can thus place significant amounts from criminal activities, especially in the case of autonomous betting terminals;
- awarding fictitious winnings to certain players or fictitious cancellation of betting tickets after they have actually been validated as non-winning in the betting system;
- the absence of appropriate KYC policies;
- participation in the game through intermediaries; (eg: through an informal system of value transfer that generally takes place through non-banking financial institutions or other commercial entities whose main business activity is not represented by the transmission of money such as hawala);
- betting ticket cancellation policy;
- complicity of employees in carrying out illegal actions.

C. SLOT MACHINES

In relation to slot machine gambling activity, risks could include:

- presence of cash transactions;
- the autonomy of the presence of slot-machine type game means assuming as many opportunities to place and withdraw some funds of suspicious origin;
- concealment of the identity of the real beneficiaries/participation in the game through intermediaries;
- the presence of clients from economic-geographic areas with high ML/TF risk;
- fictitiously awarded cash prizes/bonuses;
- players reluctant to provide information;
- loyalty programs involving cash rewards;
- casual players, including tourists;
- complicity of employees in carrying out illegal actions;
- player credit.

D. REMOTE GAMING (Casino, Betting, Slot-machine, Poker, Bingo)

In relation to remote gambling activity, a number of risks associated with the lack of face-to-face contact due to the use of the internet have been identified, as well as other risks which may include:

- the lack of physical presence of the players - impediment in getting to know the clientele and increasing the degree of anonymity;
- remote gambling used as a front for cash deposits, then transferred to bank accounts, originating apparent gambling winnings;
- involving a high volume of transactions and financial flows;
- players' use of false or stolen identity documents;
- deficiencies in customer due diligence policies;
- the use of electronic means of payment or virtual currencies whose holders are more difficult to track on the online platform;
- E-Wallet – payment method that makes it difficult for the operator to identify the owners of the funds;
- the activity of organizing and exploiting remote gambling carried out by criminal groups;

General vulnerability of the sector and specific products to the risk of money laundering

In the field of gambling service providers, the following relevant indicators represent gambling system vulnerabilities:

a) Online gambling:
- the low level of transparency regarding the identity of the customer or the beneficial owner involved in some products, services, transactions or distribution channels offered;
- the situations in which the way in which the activity is carried out allows the customer or the real beneficiary to remain anonymous;
- very short time intervals between the initiation and completion of the transaction;
- the use of innovative products, especially technologies or payment methods whose operation is not transparent or not sufficiently described (new trends in gambling are online casinos using cryptocurrencies and electronic wallets).
- physical absence of the customer for identification purposes;
- use of stolen identities;
- difficulties in identifying clients whose physical presence is not possible;

b) Terrestrial gambling
- casual players, including tourists, could present a risk, in situations where there would be deviations from their normal behavior, taking into account the standard player profile;
- players who spend significant amounts (big players), which is a risk factor given the difficulty in assessing the legal origin of funds.
- transactions that take place predominantly in cash;
- the value or volume of transactions and the complexity of products, services or transactions that could generate an insufficient level of monitoring or make it difficult to apply customer due diligence measures;
- interaction between clients from different jurisdictions;
- products or services that by their nature encourage high value transactions;
- the absence of maximum limits applicable to transactions, which would prevent the use of the product or service for the purpose of money laundering or terrorist financing;

In casinos, an established method is where criminals use large amounts of cash to purchase chips, but engage in minimal bets. After a while, they give up the game, exchange their tokens for cash or other payment instruments, assuming any insignificant losses. From the point of view of the activity carried out in a casino, this customer behavior is illogical.

The launderer may also use intermediaries, either to make cash transactions or to run the actual game, so as not to draw attention to very large sums at the disposal of a single person.

In international practice, other methods of money laundering through casinos have been identified, such as: - the purchase by money launderers of some tokens, at a higher price than the casino's, from various other players with a "clean" history; using tokens as exchange currency to purchase products that are prohibited (e.g. drugs); afterwards, the traffickers can go to the casino to convert those chips (received as payment for the drugs) into cash.

However, serious problems arise with online casinos, which allow players to play casino games from the comfort of their homes, with the only requirement being access to the internet, either through a computer or mobile phone, without any control on the source of the funds involved.

Speculating on the opportunities offered by this system, numerous members of criminal groups can launder dirty money by depositing into open accounts via the Internet and after a few gaming sessions claim that the so-called winnings are sent to the account opened on the respective gaming platform.

Fit&proper mechanisms, registration/authorization and surveillance mechanisms

Risk mitigation measures applied by ONJN - an institution with regulatory, sectoral supervision and control role for the games of chance market

According to the legal regulations in force[82], in order to obtain a license for the organization of games of chance, for class I authorization (Traditional Gambling and Remote Gambling), the legislation provides for a series of conditions imposed on the legal representatives/associates/administrators/real beneficiaries of the legal entity, so that the regulatory authority ensures that they are suitable and competent persons[83] which may protect those entities against their misuse for criminal purposes, as well as conditions on the legal person applying for the licence, such as:

- the existence of the opinion of the police bodies granted to the legal representatives, as well as to the associates/shareholders of the legal entity;
- the legal representatives/associates/administrators are required to have a criminal record certificate or other document issued by the competent authorities showing that no final judgment of conviction has been issued against them for which rehabilitation has not taken place, in Romania or in a state foreigner, for a crime provided for by GEO no. 77/2009 or for another crime committed with intent for which a minimum 2-year prison sentence was imposed;
- the economic operator is requested the tax certification certificate, as well as a sworn statement of the legal representative/authorized representative which indicates that he was not convicted by a final decision for which rehabilitation did not take place;
- the legal representatives of the legal entity must submit an affidavit stating:

- that no administrative measures have been taken against the legal entity or its representatives - such as cancellation, revocation or suspension of the license or authorization - in the field of gambling or is not in the procedure of applying some administrative measures[84], for a period of one year before the date of submitting the application for obtaining the license;

- the identity of the real beneficiaries[85] as well as the fact that they have not been convicted by a final judgment for which rehabilitation has not intervened for an offence provided for by GEO No 77/2009 or for another offence committed with intent for which a sentence of at least 2 years' imprisonment has been imposed and are not in a state of incompatibility as regulated by law.

[82]According to GD 77, art 15,
[83]Conf. art. 31 para. (2) from Law no. 129/2019
[84]in accordance with the provisions of GEO 77/2009,
[85]as defined in Law no. 129/2019

In relation to remote gambling, in addition to the requirements imposed on the legal representatives/associates/administrators/beneficial owners of the legal entity, so that the regulatory authority ensures that they are suitable and competent persons who can protect those entities against the use their abusive use for criminal purposes, the legislation provides a series of additional conditions to ensure the fulfillment of all requirements regarding customer knowledge, such as:

- that they have a bank account for depositing players' funds opened at a bank in Romania;
- that the central computer system of the organizer has a system for registering and identifying the participants in the game, as well as a system for keeping and transmitting in real time to a mirror server and a safety server, located on the territory of Romania and made available free of charge ONJN, of the fee game sessions placed by each player, as well as the winnings paid to each player;
- that the game server and the security server ensure the storage of all data regarding the provision of remote gambling services, including registration and identification of players, bets placed and winnings paid, data that must be stored for a minimum period of 5 years;
- that the communications equipment and the central point where the organizer's central IT system will be located are on the territory of Romania or on the territory of another member state of the European Union or on the territory of another member state of the Agreement on the European Economic Area or in the Swiss Confederation;
- means of payment used and monetary means, including cards, must be operated through a payment processor licensed by ONJN.

On the ONJN website one can consult the list containing all licensed operators, respectively: gambling operators who hold a license to organize games of chance (valid for 10 years), the sites and companies that have the right to promote the activities of online gambling, software providers and other services relevant to the sector. In the list above you can find: the name of each operator, the types of games of chance it can legally offer, the date until when the license is valid.

For remote gambling, the updated list of websites licensed by the ONJN can be accessed on the official ONJN website. In Romania you can only gamble legally on sites licensed by ONJN. Access to other gambling websites is strictly forbidden. If individuals access an unlicensed gambling operator for gambling purposes, the fine they may receive is between RON 5,000 and RON 10,000[14].

It is also important to note that there is a list (blacklist) on the ONJN website[86] which includes 1333 gambling sites that are not legal to play on. Internet providers are obliged to block access to these illegal sites, but there are still a multitude of such sites that can be accessed from certain IPs in our country. The companies were warned not to allow the game to players who access the sites from Romanian IPs or to Romanian players according to the legal provisions and to return to the players the existing money in the game account.

During discussions in the Focus Groups convened for the purpose of this risk assessment, issues were raised about licensing procedures that do not contain adequate measures

[86] (http://onjn.gov.ro/lista-neagra/)

regarding the beneficial owners of the entities applying for licensing. Also, the procedure does not provide for a complex verification in relation to the real beneficiary.

USE OF ACCOUNTS HELD IN ROMANIA BY LEGAL ENTITIES RESIDENTS CARRYING OUT THEIR ACTIVITY IN THE GAMBLING SECTOR FOR THE RECYCLING OF FUNDS FROM CRIMES COMMITTED IN OTHER COUNTRIES	
Description	The typology is characterized by the presence of a group of non-resident legal persons, registered in countries with a high risk of money laundering, who transferred money to the accounts of resident legal persons, and the latter either transferred the money to individuals with influence in the gambling sector or withdrew the funds in cash. The money transferred by non-resident legal persons originated from transfers ordered by resident gambling entities (involved in tax evasion operations). This created the possibility that the real beneficiaries of gambling companies could come into possession of large sums of money that came from untaxed, untaxed and other illegal activities.
Profile of natural Person/legal entity	Resident individuals holding managerial positions in state institutions with a supervisory role in the gambling sector. Residence of legal persons in areas considered to be at risk of money laundering. Entities operating in the gambling sector. The field of activity of the resident legal persons who received money from external transfers was that of consultancy services, which allowed the easy transfer of large sums of money on the basis of supporting documents that were difficult to verify in terms of veracity.
Indicators (type-specific)	- repeated foreign receipts from the same non-resident company registered in a high-risk country; - the concordance between the credits and debits of an account on the same day or in the following days; - the purchase with the collected sums of luxury goods and tourist packages; - making frequent and substantial transfers of funds by the non-resident legal entity, operations whose purpose cannot be identified as having an economic justification;
MECHANISM	• using the account of a legal person to carry out transactions involving amounts from untaxed commercial activities; • using the accountof a legal person in order to transfer sums of money to individuals; • using the account of a legal entity as transit accounts.
INSTRUMENT	• the use of external transfers; • use of cash; • use of bank accounts;

Conclusions:

The exposure of the games of chance service provider sector to the risk of money laundering is mitigated by a number of factors such as:

- the sector is well regulated in terms of the legal framework in force;

- the supervision and control of the way of applying the legislation in the field of AML/CTF are ensured by the NOPCML and the ONJN, an institution responsible with regulating, sectoral supervision and control of the games of chance market;
- both NOPCML and ONJN have the power to impose sanctions for AML/CTF violations.
- the existence of fit&proper mechanisms, respectively legal regulations in force[87] imposing a number of conditions on the legal representatives/partners/managers/real beneficiaries of gambling service providers so that the regulator can ensure that they are fit and proper persons[88] *which can protect those entities against their misuse for criminal purposes;*
- the NOPCML offers training seminars intended for games of chance service providers;

The games of cjance service provider sector presents some vulnerabilities such as:
• some of the services the sector offers can be attractive to money launderers.
•the degree of awareness of the sector regarding the risks of ML/TF still appears to be limited given the low level of reporting of suspicious transactions;

In addition to the general aspects presented previously, taking into account the specificity of each category of gambling service providers, each of them was evaluated, being given a degree of risk, as follows:

Regarding BINGO games, taking into account the reduced activity carried out by only six authorized operators (this type of game of chance is no longer preferred by gamblers), it can be appreciated that BINGO games have a low risk of money laundering or terrorist financing.

At the same time, regarding the National Lottery, considering the fact that: the risk of the services offered by this type of game is low, it is owned by the state, it is properly regulated, directly by the supervisory authority, and the rules regarding the fight against money laundering and the financing of terrorism are properly applied, the risk for Lottery games of chance is considered low.

Regarding betting games and slot machines, considering the fact that: mostly cash is used, the identity of the real beneficiaries/game participants can be easily disguised and at the same time in this type of games of chance casual players could participate, making it difficult to identify them, but considering the relatively small amounts played, for these types of gambling activities the risk is considered medium.

Regarding casinos, although the risks presented in the casino section remain quite high, the inclusion of casinos, for quite a long time, in the regulatory framework on preventing and combating money laundering, as reporting entities, has had the effect of increasing the level awareness of the sector's vulnerability to money laundering. However, there are still weaknesses in the implementation of the requirements on preventing and combating money laundering and terrorist financing.

[87]According to GD 77, art 15,
[88]according to art. 31 para. (2) from Law no. 129/2019

Deficiencies were also identified within the sector's surveillance activities regarding the implementation of the requirements regarding the prevention and control of money laundering and terrorism financing, with an emphasis on the following aspects: deficiencies regarding the application, on a risk basis, of standard KYC measures, simplified or additional, which will allow them to identify, whenever necessary, the real beneficiary, non-compliance with the obligation to report to NOPCML, operations with amounts in cash, in lei or in foreign currency , whose minimum limit is the equivalent in lei of EUR 15,000 and non-compliance with the obligation to identify the client and to keep a copy of the document as proof of identity.

In this context, the level of money laundering risk related to casinos is considered high.

No.	Elements	Likelihood Rating (L)	Assessment of consequences (C)	Risk rating
	Risk in the casino sector	**Average**	**Major**	**High**
Associated vulnerabilities: **Use of cash;** **A low level of awareness regarding the risks of ML/TF and the detection of suspicious transactions;** **Deficiencies identified, within the sector's surveillance activities** **Some of the services the sector provides can be attractive to money launderers.**				
Associated threat: **Capitalizing on the opportunities offered by this sector, criminals can launder dirty money from crimes, including crimes committed abroad, for example funds from tax evasion, etc.**				
Event description: ***Mining tokens as a currency for the purchase of prohibited products (e.g. drugs)*** ***Carrying out loan-sharking activities on the premises of gambling organizers*** ***Criminals may try to hide illicit income by disguising it as casino winnings***				
Risk description: ***High risk*** ***Average probability*** ***Major consequences***				

Online gambling is an attractive tool for laundering the proceeds of crime, which requires an average level of experience, as illegal proceeds can easily be converted into legitimate gambling winnings. At the same time, gambling using virtual currencies can be attractive to cybercriminals. In this context, the level of vulnerability to money laundering in relation to online gambling is considered high.

Despite several risk-based measures already in place by many online operators, exposure to money laundering risk in online gambling is still high, as it includes significant factors such as the lack of physical presence of players, huge volumes and complex transactions and financial flows. Although it is not based on cash, it is closely related to the use of electronic currency and virtual currencies, which increases the degree of anonymity for players.

At the same time, although online gambling operators have started to develop a level of self-regulation and risk assessment, based on the processed questionnaires, it emerged that the entities that were part of the analyzed sample demonstrate that most of them have elusive general knowledge about in the field of combating money laundering and terrorist financing, and I do not know in depth the legislation that applies in the field.

Risk mitigating factors in the remote gambling sector:

For remote gambling, in addition to the requirements imposed so that the regulatory authority ensures that the legal representatives/associates/administrators/beneficial beneficiaries of the legal entity are suitable and competent persons who can protect those entities against their misuse for criminal purposes, the legislation provides a series of additional conditions to ensure the fulfillment of all requirements regarding customer knowledge.

No.	Elements	Likelihood Rating (L)	Assessment of consequences (C)	Risk rating
	Risk in the online gambling sector	**Very high**	**Moderate**	**High**
Associated vulnerabilities: **The lack of physical presence of the players, a fact that can have the effect of a poor application of KYC measures.** **Significant and complex volumes of transactions and financial flows.** **Online gambling is an attractive tool for laundering the proceeds of crime, as illegal proceeds can easily be converted into legitimate gambling winnings.** **The possibility, in some cases, of the use by the customers of online gambling operators of virtual currency or electronic wallet, which may have the effect of making it difficult for the operator to identify the source of the funds.**				
Associated threat: ***Gambling using virtual currencies can be attractive to cybercriminals (phishing, fraud, cybercrime, fraud, etc.)***				
Event description: **Illicit funds obtained from the commission of crimes can be used by resident/non-resident individuals in the online gambling sector to convert illegal proceeds into legitimate gambling winnings.**				
Risk description: ***High risk*** ***Very high probability*** ***Moderate consequences***				

4.7.2 Auditors

General description

The relevant legal framework[89] regarding the financial audit and the independent exercise of the profession of financial auditor by the persons who have acquired this quality under the conditions provided by law contains provisions according to which the financial audit consists, mainly, of the following activities:

a) the statutory audit of the annual financial statements and the annual consolidated financial statements, in accordance with the law;

b) the audit of the annual financial statements and the consolidated annual financial statements, to the extent that this does not constitute a statutory audit, in accordance with the law;

c) review engagements of the annual financial statements, consolidated financial statements and interim financial statements;

d) assurance engagements and other engagements and professional services in accordance with international standards in this field and other regulations adopted by the Chamber;

e) internal audit, other than internal public audit.

[89]GEO no. 75/1999 (republished) regarding financial audit activity

Financial auditors and audit firms may also carry out other activities[90], such as:

a) financial-accounting consultancy;
b) financial-accounting management;
c) specialized professional training in the field;
d) accounting expertise, valuation, judicial reorganization and liquidation, as well as tax consultancy.

In the reference period, the total number of entities regulated by CAFR (Romanian Chamber of Financial Auditors) is as follows:

	2018	2019	2020
No. of members natural persons - financial auditors	4,668	4,570	4,547
No. of legal person members - audit firms	1,005	1,013	1,019

The turnover of the financial audit sector –without breakdown by type of activity and by type of transaction (cash, virtual currency, bank transfer, lei, foreign currency) is as follows:

a) **2018:** 388,355,309 lei
b) **2019:** 457,434,858 lei
c) **2020:** 527,413,842 lei

Audit firms (legal entities subject to the obligation to register in the trade register) have the obligation to:

- to submit a statement regarding the real beneficiary of the legal entity, in order to be registered in the Register of real beneficiaries of the companies;
- identify the beneficial owner of customers and take reasonable steps to verify their identity so that the reporting entity is satisfied that it has identified the beneficial owner and understands the ownership and control structure of the customer. In order to meet the requirements relating to the application of due diligence measures relating to the beneficial owner, audit firms will not rely solely on the central register and will adopt a risk-based approach.

Depending on the size and nature of the business, reporting entities that meet the conditions laid down in the regulations[91] are required to provide an independent audit function for the purpose of testing policies, internal rules, mechanisms and procedures for managing money laundering and terrorist financing risks. In this context, it should be noted that the Romanian Chamber of Financial Auditors (CAFR) has issued a series of Recommendations on the audit of activities to prevent and combat money laundering (Audit AML)[92], together with the AML Audit Report Model. Based on the adopted regulations, CAFR carried out inspections during which compliance by its members with the provisions of the legislation on the prevention and control of money laundering was verified.

[90] Financial auditors and audit firms that have the quality of financial auditor can carry out the activities of accounting expertise, assessment, judicial reorganization and liquidation, as well as tax consultancy, only after acquiring, in accordance with the law, the quality of expert accountant, evaluator, insolvency practitioner or tax consultant, as the case may be, and registration as members in the organizations that coordinate the respective liberal professions." (art. 3, para. (4) of GEO 75/1999, republished)

[91] According to Article 9 of the RULES implementing the provisions of Law no. 129/2019 approved by Order of the President of theNOPCML no. 37/2021, the reporting entities supervised and controlled by the Office.

[92] https://www.cafr.ro/recomandari-privind-auditul-activitatilor-de-prevenire-si-combatere-a-spalarii-banilor-audit-aml-efectuat-in-aplicarea-prevederilor-legii-129-2019-cu-modificarile-si-completarile-ulterioare/

During the analyzed period, NOPCML received a very low number of STR from auditors. The analysis of data and information in this Report highlighted the fact that auditors were not identified as a distinct field in the case of convictions.

In the period 2018-2020, NOPCML carried out supervision and control activities for companies registered in the register of CAFR members (in which the members of the chamber are registered), as follows:

a) A number of 556 entities registered in the Register of CAFR members - audit firms - were supervised off-site, on a risk basis. After analyzing and processing the data and related information, based on a scoring system, it turned out that 8.63% presented a high risk and 5.21% presented a partially high risk.

b) During the reference period, a number of 45 entities[93] registered in the Register of CAFR members - audit firms were supervised on-site - on the spot (controlled), during some of the verification actions, it was found that the provisions were not properly applied the legislation on the prevention and combating of ML/TF (respectively in the case of 75.5% of the total audited entities it was necessary to formulate specific recommendations in the control document, and 20.58% of the total companies that received recommendations were sanctioned by contravention), the respective deficiencies being predominantly related to:

- ➢ the obligation to adopt some measures to prevent ML/TF and, for this purpose, on a risk basis, the application of measures to know the clientele that allow the identification, as the case may be, of the real beneficiary[94] (representing a weight of 40% of the total sanctions applied);

- the designation of one or more persons who have responsibilities in law enforcement / the obligation to establish appropriate policies and procedures in terms of knowing the clientele, reporting, keeping secondary or operative records, internal control, risk assessment and management, risk management compliance and communication, ensuring appropriate employee training[95](representing a weight of 20% of the total sanctions applied);
- how to implement international sanctions[96], including keeping proof of carrying out specific checks using the information available on the NOPCML website – INTERNATIONAL SANCTIONS section (representing a weight of 40% of the total sanctions applied)
- the money laundering/terrorist financing risk assessment, the risk indicators used in that assessment

[93] Of these 45 audit firms:

✓ 18 legal entities are registered both in the Register of CAFR members - audit firms and in the Register of tax consultancy firms and in the CECCAR Members' Register - legal entities.

✓ 15 legal entities are registered only in the Register of CAFR members - audit firms

✓ 9 legal entities are registered both in the CAFR Register of Members - audit firms and in the CECCAR Register of Members - legal entities

✓ 3 legal entities are registered both in the Register of CAFR members - audit firms and in the Register of tax consultancy firms

[94] Article 11 of Law No 656/2002 rep.

[95]Art. 20 of Law no. 656/2002 rep.

[96]Failure to comply with the provisions of art. 6 of the Rules regarding the supervision by NOPCML of the implementation of the international sanctions approved by GD 603/2011.

- appropriate establishment within the Internal Procedures/Norms of anomaly indicators for recognizing suspicious transactions, ➢ employee training.

In 2018-2020, the CAFR, through its specialized department, carried out controls on compliance with regulations on preventing and combating money laundering and terrorist financing. Inspectors of the structure specialized in carrying out quality controls within the CAFR's Monitoring, Control, Competence and Professional Research Compartment (CMCCCP) have checked a number of objectives concerning several aspects set out in the regulations in the field of preventing and combating money laundering and terrorist financing. During the reporting period, inspections were carried out on the compliance of the members of the CAFR with the provisions of the legislation on preventing and combating money laundering. The main deficiencies found in the period 2018-2019 with regard to non-compliance with legal provisions in the field of prevention and combating money laundering were in relation to financial auditors who:

- they did not document the classification of clients according to the identified risks;
- they did not apply the necessary measures, depending on the risks associated with each client, namely standard measures, simplified measures or additional measures;
- they did not carry out the verifications required by the legislation in force regarding international sanctions, especially in the case of legal entities whose shareholders/associates are foreign citizens;
- they did not ensure the training of employees regarding the prevention and combating of money laundering and the financing of terrorism, through training programs;
- they failed to apply know-your-customer policies and procedures and identify the beneficial owner for each customer;
- the anti-money laundering policies and procedures did not specify that information regarding customer identification will be kept for a period of at least 5 years;
- they have not developed internal procedures in order to comply with the legislative provisions in this field, included in their own quality control system implemented by the financial auditor;
- they have not designated, through an internal act, the person responsible for the implementation of the provisions relating to the prevention and combating of money laundering.

The financial auditors inspected by the Professional Monitoring, Control, Competence and Research Department (CMCCCP) in the years 2018, 2019 and 2020 did not identify during the audit missions carried out any transactions on which they had suspicions that they had the purpose of money laundering or financing terrorism[97].

In the 2018-2020 period, CAFR did not apply specific sanctions to members regarding the denial of access to the activity or suspensions/exclusions from the activity.

Anti-money laundering training:

NOPCML organized in collaboration with CAFR training sessions intended for financial auditors, the theme of the sessions had in mind: practical aspects regarding the application of legal provisions in the field of AML/CTF, types of ML/TF, implementation of the international sanctions regime.

[97]According to CAFR activity reports

From the processed questionnaires it emerged that the entities that were part of the analyzed sample demonstrate that most of them have elusive general knowledge regarding the field of preventing and combating money laundering and terrorist financing and do not have in-depth knowledge of the applicable legislation in this field.

General risks of the sector

The lack of suspicious transaction reports from entities in the audit services sector may indicate problems with the efficiency of certain enforcement mechanisms of some instruments for the implementation of legal provisions in the field of ML/TF and, in many cases, a superficial knowledge by auditors of the obligations what is due to them under the respective legislation.

Although the professional skills imposed on specialists in the field are a tool that can facilitate the identification within the audit missions of some atypical operations in relation to the current activities of the audited commercial company or some transfers that apparently have no economic or legal purpose, there is a risk that the criminals to request the complicity of the auditors or to exploit the insufficient submission by them of the diligences that can lead to the identification and reporting of suspicious transactions.

General risks of the products/services offered in the sector

The fact that financial auditors and audit firms can also provide other types of services, such as financial-accounting consultancy, accounting expertise, valuation, judicial reorganization and liquidation, tax consultancy, etc., involve risks in the sense that criminals could request a package of services from professionals to try to identify the optimal way to conceal the illicit origin of some assets.

Some of the specific services offered by the sector, namely the verification and analysis of financial statements or some of their components, carried out as part of audit missions, may in certain situations highlight suspicions of money laundering and/or predicate offenses committed by clients generators of illicit funds (for example tax evasion, other economic-financial crimes), with the risk that the criminals will try by various means to get the financial auditor not to report the respective suspicious activities.

The overall vulnerability of the sector/specific products (services) to the risk of money laundering

Vulnerabilities in terms of preventive measures identified within the supervision activities of the audit sector mainly come from the finding of non-compliance with certain legal provisions in the field, with an emphasis on the following aspects:

- failure to properly apply, on a risk basis, customer due diligence measures to also identify the real beneficiary of all customers;
- deficiencies related to the risk-based assessment process from the point of view of money laundering/terrorist financing, the appropriate establishment of the risk indicators used in the respective assessment and the application of customer awareness measures through risk-based circumstantial evidence;
- inadequacies regarding the proper training of employees regarding the provisions of the legislation regarding the prevention and combating of money laundering and the financing of terrorism, as well as regarding aspects that could facilitate their recognition of suspicious transactions;

- deficiencies in establishing/completing/updating/reassessing, within the internal procedures, anomaly indicators for the recognition of suspicious transactions;
- deficiencies in the application of legal provisions on international sanctions.

Fit&proper mechanisms, registration/authorization and oversight mechanisms

NOPCML and CAFR supervise and control the financial auditors on how they implement the provisions of the law regarding the prevention and control of money laundering and terrorism financing.

The statutory audit is carried out by financial auditors or audit firms that are authorized/authorized in Romania, that are registered as members of CAFR and that are registered in the Electronic Public Registry.

CAFR registers financial auditors and audit firms based on Authorization Orders issued by the Authority for the Public Supervision of Statutory Audit Activity (hereinafter referred to as ASPAAS). According to ASPAAS Norms as well as to Law no. 162/2017, in order to get an authorization it is necessary, among other things, that the auditor or the audit firm has a good reputation. The authorization of a financial auditor or an audit firm is withdrawn[98] if the good reputation of this person or the company has been seriously compromised, among the listed situations being included:

a) the said person was convicted for committing a crime with intent;
b) against the natural person, a preventive measure depriving or restricting freedom was taken in the framework of a criminal trial, in the event that investigations are carried out under the aspect of committing a crime with intent.

For auditors, the assessment of internal controls and procedures to prevent and combat money laundering and terrorist financing is part of the due diligence procedures for the integrity of the profession.

USE OF ACCOUNTS HELD IN ROMANIA BY A LEGAL ENTITY RESIDENT, WHO CARRIES OUT ITS ACTIVITY IN THE FIELD OF INVESTMENTS, FOR OUTSOURCING MONEY OBTAINED FROM FRAUDULENT BANKRUPTCY	
Description	The typology is characterized by the presence of a group of non-resident legal entities, registered in countries with a high risk of money laundering, who receive large sums of money from a resident company operating in the field of investments, the transfers being made on the basis of contracts international insurance.
Profile of natural persons /legal entities	The resident legal entity was involved in committing the crime of fraudulent bankruptcy, acting as an investor. The resident legal entity is controlled by a resident natural person who has carried out a long-term activity in the field of investments. The non-resident legal entities, beneficiaries of the funds, were registered in countries with a non-cooperative banking system.

[98] Art 6 of LAW no. 162/2017 regarding the statutory audit of annual financial statements and consolidated annual financial statements and amending some normative acts

Indicators (type-specific)	- the auditor's verification of the reality of the insurance contracts and related deposits, which led to the conclusion that the deposits submitted by the insurers were fictitious; - external transfers were justified by fictitious documents; - the transfers made by the resident legal entity to the associate were not economically justified.
MECHANISM	• using resident legal entity accounts to make external transfers to countries with non-cooperative banking systems; during the audit mission, the auditor had an overview of the activity of the audited entity, so that he could identify suspicious transactions; • the use of accounts belonging to resident natural persons for the transit of sums of money coming from resident legal persons.
INSTRUMENT	• the use of external transfers; • use of bank accounts.

Conclusion:

As there are some weaknesses in the way this category of reporting entities carry out checks and manage risks, the level of money laundering vulnerability associated with the services provided by the auditors is assessed as low, given that the auditors are well organized in terms of from the point of view of the legal framework applicable to the profession, the attributions and the important role assumed by the CAFR, the way in which the auditors carry out their activity and the type of services offered are factors that reduce the level of vulnerability.

NOPCML carried out a limited number of inspections, therefore a relatively small number of deficiencies were identified. However, the sector is well supervised by the CAFR, as evidenced by the significant number of controls carried out.

In addition, the inherent risk of the activities carried out is low due to the nature of the services provided by the auditors.

No.	Elements	Likelihood Rating (L)	Assessment of consequences (C)	Risk rating
	The risk to auditors	**Low**	**Moderate**	**Low**
Associated vulnerabilities: **Some shortcomings in the application of anti-money laundering and anti-terrorist financing legislation.**				
Associated threat: **Concealment of the proceeds of crime.**				
Event description: **insufficient practice of a risk-based approach during the assessments/monitoring carried out and the measures applied**				
Risk description: ***Low risk*** ***Low probability*** ***Moderate consequences***				

4.7.3 Chartered accountants and accounting experts

General description

NOPCML and CECCAR supervise and control chartered accountants and accounting experts regarding the application of the provisions of the law for the prevention and combating of money laundering and terrorist financing.

The Body of Chartered Accountants and Accounting experts in Romania (hereinafter referred to as CECCAR) is the professional organization without patrimonial purpose, an autonomous legal entity of public utility which includes chartered accountants and accounting experts. This is the only competent authority that organizes and monitors the activity of accounting experts and chartered accountants, as well as accounting and accounting expertise companies, respectively accounting companies.

Access to the profession is conditioned by the fulfillment of certain requirements, including that the natural person has not suffered any conviction which, according to the legislation in force, prohibits the right to manage and administer companies. Also, the annual visa for the exercise of the profession by accounting experts and chartered accountants is granted to them only if they cumulatively meet certain conditions, including the proof that they have not suffered any conviction which, according to the legislation in force, prohibits the right to manage and administer commercial companies (presentation of criminal record certificate or sworn statement).
In the List of accounting experts and chartered accountants in Romania, the persons holding the quality of chartered accountant and accounting expert are registered; all members, natural persons, accounting experts, separately from chartered accountants, as well as profile companies, grouped according to the territorial criterion, are entered in the membership List.

According to the provisions of the relevant legal framework[99] regulation of this activity, regarding the services provided within this sector, we specify that:

A. **The accounting expert** can perform, as an individual professional or as a registered company, both for individuals and for legal entities, the following works:
   a) organizes, manages, keeps, verifies and supervises the accounting, prepares and signs the financial statements and performs fiscal works, namely the calculation of taxes, fees and contributions, the preparation and submission of fiscal declarations and ensures the representation of the client in the relationship with the tax authorities, as part of a service contract in the field of accounting;
   b) provides specialized assistance regarding the organization and book keeping;
   c) performs economic-financial analyses and assessments for financial-accounting purposes, according to the law; such assessments may refer to estimates of cash flows and of the entity's financial condition, assessment of income and expenses, estimation of the level of provisions and value adjustments, as well as other assessments performed by accounting experts in their current activity, without limiting to these;
   d) performs financial-accounting expertise, including financial-accounting expertise with a fiscal component, ordered by judicial bodies or requested by natural or legal persons under the conditions provided by law and CECCAR regulations;

[99]Government Ordinance no. 65/1994 on the organization of the activity of accounting expertise and authorized accountants with subsequent amendments

e) performs other financial-accounting works, including electronic staff records, payroll, administrative and IT organization activities, certification of information, data and documents;
f) fulfills, according to the legal provisions, the duties provided for in the mandate of censor and financial trustee;
g) provides the specialized assistance necessary for the establishment and reorganization of companies;
h) ensures financial-accounting management and economic performance;
i) ensures internal management control and risk management of legal entities;
j) provides consultancy in financial management and accounting, provides services specific to managerial accounting and integrated reporting;
k) performs professional services for individuals and legal entities that require knowledge of the above-mentioned activities.

Accounting experts can practice their profession individually or they can form accounting and/or accounting expertise companies. Accounting expertise companies and accounting companies must meet the conditions listed by the legislation in the field.

B. **Chartered accountants** can perform the following works for either individuals or legal entities:
a) keep the accounting of the economic-financial operations provided for in the contract;
b) prepare financial statements;
c) perform electronic personnel record and payroll activities.

Chartered accountants can practice their profession individually or they can be incorporated in accounting companies, established according to the law.
Accounting companies (legal entities subject to the obligation to register in the Trade Register) have the following obligations:
- to submit a declaration regarding the real beneficiary of the legal entity, in order to be registered in the Register of real beneficiaries of the companies, in compliance with the legal provisions in force;
- to identify the beneficial owner of clients and take reasonable steps to verify their identity so that the reporting entity is satisfied that it has identified the beneficial owner and understood the ownership and control structure of the client. In order to fulfill the requirements related to the application of KYC measures related to the beneficial owner, the reporting entities will not rely exclusively on the central register; these requirements are considered to be met using a risk-based approach.

The analysis of the STRs revealed that accounting experts and chartered accountants were not identified as a distinct sector.

The analysis carried out by the authorities highlighted the fact that among the money laundering channels used most often is the use of accounting specialists. The typologies analyzed refer to aspects regarding various connections with the activity carried out by accountants and some predicate crimes (premise crimes from which the money subjected to the laundering action originates), for example:
- the registration in the accounting of companies controlled by criminals of some fictitious invoices issued by companies with ghost behavior (in order to unrealistically increase expenses);

- failure to register in the accounting of some companies the operations carried out and the income obtained from the sale of some goods;
- the drawing up of fictitious invoices certifying the sale of goods to several companies with ghost behavior, in this way trying to hide some criminal activities;
- the registration of some invoices in the accounting and the collection of their consideration for services that were not actually provided;
- the creation of fictitious financial circuits, consisting in the recording in accounting and settlement of expenses for goods and services, for the benefit of private legal entities, which, in reality, did not fulfill the obligations for which they were paid.

In the period between 2018 – 2020, NOPCML carried out risk-based off-site surveillance activities for 3,340 entities registered in the CECCAR Membership List of legal entities, following the analysis and processing of related data and information, based on a scoring system, resulting in 2.36% of the entities being classified as high risk.

During the reporting period, 77 entities registered in the CECCAR Membership List were supervised on-site (verified), as a result of the on-site control actions carried out by NOPCML a number of breaches of the legal provisions in the field of AML/CTF were identified, the control teams carried out training of the legal representatives of the entities checked on the best ways of complying with the legal framework in this matter, and appropriate fines were imposed (in the case of 33.76% of all firms verified) and recommendations were recorded (in the case of 79.22% of all firms checked) to remedy the infringements found concerning:

- non-compliance regarding the application of KYC measures so as to allow the identification of the real beneficiary, if necessary;
- non-compliance regarding the updating/completion of internal procedures with specific provisions regarding: the risk-based assessment process from the point of view of ML/TF, the risk indicators used in that assessment and the application of measures to know the clientele through risk-based circumstantiation;
- non-compliance with the designation of one or more persons who have responsibilities in the application of legislation in the field of prevention/control of ML/TF and the duties entrusted in this regard;
- non-compliance with the obligation to establish appropriate policies and procedures in terms of KYC, reporting, keeping secondary or operative records, internal control, risk assessment and management, compliance management and communication, ensuring the appropriate training of employees[100]
- non-compliance with aspects regarding the implementation of the legal provisions in the matter of international sanctions[101], including keeping proof of execution specific checks using the information available on the NOPCML website – INTERNATIONAL SANCTIONS section;
- non-compliance with the obligation of entities to report to NOPCML, in no more than 10 working days, the performance of operations with amounts in cash, in lei or in foreign currency, the minimum limit of which is the equivalent in lei of EUR 15,000, regardless of whether the transaction is carried out through one or more many operations that seem to be related to each other[102].

[100]Art. 20 of Law no. 656/2002 rep.

[101]Failure to comply with the provisions of art. 6 of the Rules regarding the supervision by NOPCML of the implementation of international sanctions approved by GD 603/2011

[102]Art 5 paragraph (7) of Law no. 656/2002 rep.

NOPCML organized, in collaboration with CECCAR, training sessions intended for accounting experts and authorized accountants, in the period 2018-2020, the theme of the sessions taking into account: practical aspects regarding the application of legal provisions in the field of AML/CFT, types of ML/TF, implementation international sanctions regime.

From the processed questionnaires, it emerged that the entities that were part of the analyzed sample demonstrate that most of them have elusive general knowledge regarding the field of combating money laundering and terrorist financing and do not know in depth the legislation that applies in the field.

General risks of the sector

In the context where, during the preparation of analyses/reports/assessments, accounting experts/chartered accountants can detect anomaly indicators that lead to the identification and reporting of suspicious transactions, criminals can try to corrupt the specialists in this sector, or they can speculate on the situations in that they do not perform all due diligence regarding: permanent monitoring of operations, risk assessment and the application of KYC measures, depending on the size, diversity, nature and scope of the accounting services provided, the clients' field of activity and the extent of the transactions carried out by these.

Criminals could ask accountants for services that facilitate:

- the use of financial products for illicit purposes; operations such
- as
    - over/under billing of goods / services;
    - multiple billing for the same goods / services;
    - setting up companies with "opaque structures" where the true identity of the beneficial owner/beneficiary is hidden through the use of intermediaries;
- advice on carrying out transactions in such a way as to avoid their reporting to the NOPCML or for certain operations to acquire the appearance of legality (for example, the accounting registration of fictitious/unreal operations, goods/services for which there are no supporting documents, etc.).

General risks of the products/services offered in the sector

Regarding the vulnerabilities of accounting services, we exemplify:

- situations in which criminals may ask accountants for advice in order to hide, through the entities they own/control, the illicit origin of some funds/assets or to disguise the links between the income obtained from illegal activities and the perpetrator (including the interposition/establishment of companies/ legal constructions with a complex, non-transparent structure);
- situations in which the criminals ask accountants for advice on financial operations related to the sale/purchase/transfer of some properties, the analysis showing that their purpose is to conceal the transfers of illegal funds (stratification stage of the ML) or the use of these revenues, after what went through the laundry process, in making various investments (ML integration stage);
- situations where criminals may try to use accountants as intermediaries to carry out or facilitate various financial operations (for example: deposits or withdrawals of cash from bank accounts, currency exchange operations, issuing and cashing checks, buying and selling shares, making external transactions, etc.).

Overall vulnerability of the sector/specific products to the risk of money laundering

Accounting services may seem attractive to criminals, as these services could facilitate the creation of an appearance of legitimacy for funds of illicit origin. Professionals offering accounting services are at risk of being approached by criminals either for advice or for actually providing services. The lack of suspicious transaction reports from this sector is an indicator of vulnerability.

The vulnerabilities identified (within the sector's surveillance activities) in relation to the entities' application of preventive measures mainly arise from the finding of non-compliance with the legal provisions, with an emphasis on the following aspects:

- the measures to know the clientele applied do not in all situations allow the identification, as the case may be, of the real beneficiary of the customers;
- the risk-based assessment from the point of view of ML/TF was not properly carried out in several cases and deficiencies were found regarding the application of customer knowledge measures through risk-based circumstantiation and the risk indicators used;
- inadequacies regarding the proper training of employees regarding the provisions of the legislation in the field of AML/CTF and practical aspects that can facilitate their recognition of suspicious transactions (for example, the presentation of relevant case studies);
- deficiencies regarding the establishment/completion/updating/reassessment of the anomaly indicators for the recognition of suspicious transactions within the internal procedures.

During the discussion in the focus groups gathered for this risk assessment, the representatives of this profession emphasized the following aspects:

- They expressed concern about the difficulty to identify suspicious transactions and to decide when to submit a Suspicious Transaction Report (STR) to the NOPCML.
- The self-regulatory body has carried out some off-site inspections (ON-SITE) on the sector's compliance with anti-money laundering and anti-terrorist financing legislation, and in case of major non-compliance, including in relation to the conduct of internal checks/monitoring/inspections and the drafting/application of internal procedures/standards on the fulfilment of obligations under the AML/CTF legislation, CECCAR representatives considered that they could apply disciplinary sanctions and exclude such persons from the profession, but any contravention sanctions for non-compliance with the AML/CTF legislation could only be applied by NOPCML.
- CECCAR emphasized the need to provide inspectors with additional professional guidance and training in the reference field, considering the existence of gaps in relation to risk-based supervision of how the entities in the sector apply the legal provisions in the field of AML/CTF .

Conclusions:

Given that, although there are factors that mitigate the sector's exposure to money laundering risk, such as:

- the fact that the sector is well regulated in terms of the legal framework in force applicable to the profession;
- CECCAR member accountants/certified accountants have the ethical responsibility to act in the public interest;
- The supervision and control of the way of applying the legislation in the field of AML/CTF is ensured by NOPCML and by CECCAR, as a self-regulatory body for the reporting entities that they represent and coordinate;
- the existence of fit&proper mechanisms that ensure the maintenance of certain standards regarding access and retention in the profession and that prevent the access to the profession of convicted persons;
- organization by NOPCML of training seminars for professionals in the sector;

However, considering aspects such as:

- accounting services can be attractive to criminals, as these services could facilitate the creation of an appearance of legitimacy for funds having an illicit origin;
- the financial-accounting activity can be carried out as an employee and by persons without a specialization in the field and who do not hold the status of chartered accountant/accountant and are not members of the professional body;
  as a result, these people do not obey the code of ethics and deontological and professional norms, these being only applicable to CECCAR members;
- the analysis carried out by the authorities highlighted the fact that among the money laundering channels used most often is the use of accounting specialists;
- the degree of awareness of the sector regarding the risks of ML/TF still seems to be limited considering the lack of reports of suspicious transactions originating from this sector;
- the identification, within the supervision activities of the sector, of non-compliance with the legal provisions, with an emphasis on the following aspects: the KYC measures applied do not allow to identify, in every situation, as the case may be, the real beneficiary of the clients, the assessment based on risk from the point of view of ML/TF was not performed properly in several cases and deficiencies were found regarding the application of KYC measures through risk-based circumstantiation and the risk indicators used,

the level of vulnerability to money laundering, with regard to the sector, is considered significant, which led to the establishment, at national level, of a medium ML risk degree associated with the sector.

No.	Elements	Likelihood Rating (L)	Assessment of consequences (C)	Risk rating
	The risk of certified public accountants and chartered accountants	**High**	**Moderate**	**Average**
Associated vulnerabilities: **Accounting services can be attractive to criminals, as these services could facilitate the creation of an appearance of legitimacy for funds having an illicit origin;** ***The identification, within the supervision activities of the sector, of non-compliance with the legal provisions;*** **Deficiencies in detecting suspicious transactions and risk situations.**				
Associated threat: **Accounting registration of fictitious/unreal operations.**				

Event description: **Criminals can ask accountants for:** **- consultancy to hide, through the entities they own/control, the illicit origin of some funds/assets or to disguise the links between the income obtained from illegal activities and the perpetrator** **- advice on conducting transactions so that certain assets acquire the appearance of legality**
- the establishment of companies with "opaque structures" in which the true identity of the real owner/beneficiary is hidden through the use of intermediaries **-over/under-invoicing of goods/services** **-multiple billing for the same goods/services.**
Risk description: ***Medium risk*** ***High probability*** ***The consequences are moderate***

4.7.4 Authorized appraisers

General description

The profession of authorized appraiser is regulated by Government Ordinance no. 24/2011, approved by Law no. 99/2013, with subsequent amendments and additions. By the same normative act, the National Association of Authorized Appraisers in Romania, hereinafter referred to as ANEVAR, was established as a professional organization of public utility, without patrimonial purpose, the authorized appraisers are members of, also establishing the method of access to the profession of authorized appraiser.

The National Association of Authorized Appraisers in Romania (ANEVAR) is the competent authority that organizes, coordinates and authorizes the activity of authorized appraisers in Romania. The association represents the interests of the authorized appraiser profession at national and international level.

Legal entities based in Romania or in another member state of the European Union or the European Economic Area, corporate members of the Association, can carry out assessment activities.

By assessment, we mean the activity of estimating the value, materialized in a document, called an assessment report, carried out by an authorized appraiser, in accordance with the specific standards of this activity and professional ethics.

The assessment activity is compatible with the following activities:
a) business and management consulting;
b) development of financing projects;
c) assessment of financing projects;
d) accounting expertise, financial audit, judicial reorganization and liquidation, as well as tax consultancy.

The authorized appraisers, members of ANEVAR, in the independent exercise of the profession, carry out, mainly, the following activities:
a) real estate appraisal;
b) business appraisal;
c) appraisal of movable assets;

d) appraisal of shares and other financial instruments;
e) appraisal of goodwill and other intangible assets;
f) assessment report checks.

ANEVAR[103] does not hold additional information on the money laundering/terrorist financing risks associated with each of them.

Authorized appraisers, full members and corporate members, are registered in the Association Board. The situation regarding the number of ANEVAR members, from the period 2018-2020 is as follows:

a) **Full members, distributed by specialization**:
   a. In 2018 - a total of 3972 members, in 2019 - a total of 3994 members, in 2020 - a total of 3975 members who:
      i. hold the specialization Real Estate Appraiser (EPI) – in 2018 - 3598 members, in 2019 – 3669 members, in 2020 – 3661 members;
      ii. have the specialization Appraiser of business enterprises, of trade funds and other intangible assets (EI) – in 2018 – 1670 members, in 2019 – 1595 members, in 2020 – 1545 members;
      iii. hold the specialization Mobile Assets Appraiser (EBM) – in 2018 - 1572 members, in 2019 - 1576 members, in 2020 – 1627 members;
      iv. hold the specialization Assessment Report Checks (VE) - in 2018 - 119 members, in 2019 - 118 members, in 2020 - 117 members;
      v. are specialized in Stock Valuations and other Financial Instruments (EIF) – in 2018 - 38 members, in 2019 - 37 members, in 2020 - 36 members.

b) **Corporate members (they are not allocated by specialization and can carry out any type of assessment depending on the specialization of employees/collaborators) - in 2018 - 507 members, in 2019 - 519 members, in 2020 - 542 members.**

The turnover of the sector related to the period 2018-2020 was:

- In 2018, the turnover of the sector had a total value of 195,683 thousand lei, of which 79% was related to authorized appraisers specialized in real estate appraisals (EPI), and 56% was made by legal entities (companies) with this specialization. The assessments carried out in 2018, in relation to turnover, were mainly aimed at: financial reporting (32.3%), taxation (18.9%) and loan guarantees (16.17%).
- In 2019, the turnover of the sector had a total value of 213,681 thousand lei, of which 81% was related to authorized appraisers specialized in real estate appraisals (EPI), and 53.7% was made by legal entities (companies) with this specialization. The assessments carried out in 2019, in relation to the turnover, were aimed mainly at: "guaranteeing loans" (34.6%), "taxation" (18.8%) "financial reporting" (15.59%).
- In 2020, the turnover of the sector had a total value of 220,046 thousand lei, of which 82% was related to authorized appraisers specialized in real estate appraisals (EPI), and 54.5% was made by legal entities (companies) with this specialization. The assessments carried out in 2020, in relation to the turnover, were aimed mainly at: "guaranteeing loans" (33.9%), "taxation" (20.6%), "financial reporting" (15.1%)

[103] Information sent by ANEVAR

Commercial companies that have this object of activity - exercising the profession of authorized appraiser - (legal entities subject to the obligation to register in the commercial register) have the obligation:

- to submit a statement regarding the real beneficiary of the legal entity, in order to be registered in the Register of real beneficiaries of the companies;
- to identify the beneficial owner of clients and take reasonable steps to verify their identity so that the reporting entity is satisfied that it has identified the beneficial owner and understood the ownership and control structure of the customer. In order to fulfill the requirements related to the application of KYC measures related to the beneficial owner, the reporting entities will not rely exclusively on the central register; these requirements are considered to be met using a risk-based approach.

In NOPCML's case analysis module, chartered appraisers have not been identified as a distinct sector.

The analysis shows that among the specific elements of the OCG's mode of operation in Romania is included the overestimation of the market value of real estate obtained fraudulently and ending up, in different forms (e.g.: contribution to capital) in the patrimony of companies owned or controlled by intermediaries by the members of the groups in question, mortgaging them (with the complicity of authorized appraisers/bank officials) in order to obtain bank loans.
The analysis highlights the fact that appraisers are among the professionals with a significant possibility of being used in money laundering schemes.

One of ANEVAR's attributions is the monitoring of the application of the assessment standards adopted by it in carrying out the assessment activity of authorized appraisers. Along with the achievement of this attribution, the monitoring of the application by the authorized appraisers of the provisions which are opposed to them under the legislation on the prevention and combating of money laundering and the financing of terrorism is carried out. Regarding the irregularities found by ANEVAR in within the process of monitoring some members, we specify that:

- 3-5% of the corporate members inspected did not designate a person in the relationship with NOPCML, an obligation provided for in art. 23 para. (1) of Law no. 129/2019 and did not submit the name of this person to NOPCML;
- 5-7% of the inspected corporate members and approximately 10% of the inspected titular members did not institute a Procedure containing provisions on how to report to NOPCML any suspected money laundering;
- 1-2% of the regular members did not classify clients according to risk.

The processed questionnaires indicated that the entities that were part of the analyzed sample demonstrate that most of them have elusive general knowledge regarding the field of combating money laundering and terrorist financing, and they do not know in depth the legislation that applies in the field.

General risks of the sector

In general, in the context of the lack of suspicious transaction reports from the authorized appraisers sector highlighted by the analysis carried out by NOPCML, the risk exposure of the sector may consist of:

- the fact that criminals or their accomplices can request a certain outcome of the assessment, in order to use it in certain transactions with money from crimes;
- the request for assessment services by clients who fall into the high-risk category (e.g. PEP or from an area of significant geographic risk) and/or who are reluctant to provide all relevant information or in respect of which professionals have a reasonable suspicion that the information provided is incorrect or insufficient.

General risks of the products/services offered in this sector:

In relation to the services provided by authorized appraisers, some of the risks include:

- overvaluation of the market value of some assets obtained fraudulently and ending up, in various forms, in the patrimony of companies owned or controlled through intermediaries by members of criminal groups in order to obtain advantages (for example, bank loans with significant values later repaid with funds having a illicit origin or obtaining a semblance of legality for proceeds from crimes);
- the undervaluation of some assets, for example assets belonging to economic agents in which the state or a local public administration authority is a shareholder;
- valuation (not carried out in accordance with the asset valuation standards approved by law) of assets of debtors in insolvency proceedings.

General vulnerability of specific sector/products to the risk of money laundering

The monitoring carried out by ANEVAR highlighted vulnerabilities related to the sector in terms of the knowledge and application by the corporate members of the obligations regarding: the designation of a person responsible for ensuring compliance with the legislation on combating money laundering and the financing of terrorism, the development of specific procedures and the classification of clients according to of risk.

Competence and probity mechanisms (FIT&PROPER), registration/authorization and oversight mechanisms

Authorized appraisers are reporting entities supervised and controlled by NOPCML and ANEVAR regarding the application of the provisions of the legislation to prevent and control money laundering and terrorist financing.

ANEVAR is the competent authority that organizes, coordinates and authorizes the activity of an authorized appraiser in Romania. The assessment activity can be carried out only by persons who have the capacity of authorized appraiser, who are registered in the Association Board.

According to the provisions of art. 15 and of art. 16 of OG no. 24/2011, a natural person cannot acquire ANEVAR membership if (s)he is definitively convicted for committing a crime with intent. Moreover, according to art. 16 and of art. 17 of OG no. 24/2011 the ANEVAR membership shall be lost if the ANEVAR member is definitively convicted for committing a crime with intent. In order to carry out checks to fulfill the legal requirements, ANEVAR undertakes the following:

- when registering in ANEVAR, a criminal record certificate is requested;

- annually, members give a sworn statement in the appropriate section of the activity report mentioning if they have been definitively convicted of committing a crime with intent.

During 2018-2020, ANEVAR had several membership withdrawals; of these, as a result of the non-fulfillment of the requirement that the titular member not have been definitively convicted as a result of committing a crime with intent, in 2019 membership was withdrawn for 2 entities[104].

Regarding the measures applied by ANEVAR regarding the suspension of membership, in the period 2018-2020, they were not based on non-compliance with the legislation on combating money laundering and the financing of terrorism.

During the focus group discussions held for the purpose of this risk assessment, it was found that sometimes appraisers do not have a clear understanding of how they should identify suspicious transactions in the course of their work and how money laundering could be facilitated by the services offered within the sector. Industry representatives recognize the possibility that, to a limited extent, appraisal services could be misused, and highlight the need for sustained guidance on industry-specific indicators of suspiciousness and how they could prevent money laundering.

During the discussions in the thematic groups, ANEVAR stated that they had received a guide containing examples of warning signs and indicators specific to their sector.

No.	Elements	Likelihood Rating (L)	Assessment of consequences (C)	Risk rating
	The risk related to the Appraisers	**Low**	**Moderate**	**Low**
Associated vulnerabilities: **Some minor deficiencies in the application of the provisions of the legislation in the field of combating ML/TF.**				
Associated threat: **Criminals or their accomplices could request professionals to prepare appraisal reports without complying with the property appraisal standards approved by law, in order to use the said reports in various illicit activities.**				
Event description:				
Exclusively in cases where the appraiser would not be in good faith, the possibility could arise: • **the overvaluation of assets obtained by the client following the commission of crimes** • **the undervaluation of some assets, for example assets belonging to economic agents in which the state or a local public administration authority is a shareholder.**				
Risk description: ***Low risk*** ***Low probability*** ***Moderate consequences***				

4.7.5 Tax Consultants

General description

[104] Information sent by ANEVAR

Tax consultants are reporting entities that have all the obligations of reporting entities provided for by Law no. 129/2019. Natural and legal persons who provide tax or accounting consultancy had the status of reporting entities supervised and controlled by NOPCML and according to the provisions of Law no. 656/2002, during the period in which it was in force.

Ordinance no. 71/2001 (Law no. 198/2002 - for the approval of the Government Ordinance no. 71/2001 on the organization and exercise of the tax consultancy activity) with subsequent amendments and additions constitutes the legal framework regarding the organization and exercise of the tax consultancy activity as an independent activity, of to the people who have acquired this quality.

Tax consultants can carry out their activity as independent natural persons or they can associate in companies whose business is tax consultancy. The company must have at least one partner/shareholder and administrator who has the capacity of tax consultant.

Tax optimization is a way in which the taxpayer makes a choice between different solutions offered by the tax legislation for the most favorable to his own interests. However, the analysis of ML/TF vulnerabilities reveals the possibility that members of some criminal groups may use services of this type provided by the tax consultant with the aim of recycling values of illicit origin.

The analysis carried out by the authorities highlights the fact that tax consultants are among the professionals with a significant possibility of being used in money laundering schemes.

In the period 2018 – 2020, NOPCML carried out supervision and control activities for companies registered in the Register of tax consultants and tax consultancy companies as follows:

a) a number of 332 entities registered in the Register of tax consultants and tax consultancy companies were supervised off-site, on a risk basis.
Following the analysis and processing of related data and information, based on a scoring system, it was found that 20.18% presented a high risk;

b) during the reference period, a number of 66 entities registered in the Register of tax consultants and tax consultancy companies were supervised on-site (controlled);

In the case of a number of 51 of the verified entities (representing 77.27% of the total of 66 controlled entities), the appropriate non-application of the provisions of the law on the prevention and control of ML/TF was identified, and it was necessary to formulate in the control document some specific recommendations, and 22.72% of all controlled companies were sanctioned for non-compliance with the legal provisions regarding:

- the obligation to adopt measures to prevent ML/TF and, for this purpose, on a risk basis, the application of KYC measures that allow the identification, as the case may be, of the real beneficiary[105];
- the designation of one or more persons who have responsibilities in law enforcement / the obligation to establish appropriate policies and procedures in terms of knowing the clientele, reporting, keeping secondary or operative records, internal control, risk assessment and management, risk management compliance and communication, ensuring appropriate employee training[106];

[105] Art. 11 of Law no. 656/2002 rep.
[106] Art. 20 of Law no. 656/2002 rep.

- how to implement international sanctions[107], including keeping proof of carrying out specific checks using the search engines available on the NOPCML website – INTERNATIONAL SANCTIONS section.

NOPCML organized training sessions intended for tax consultants, the theme of the sessions taking into account practical aspects regarding the application of legal provisions in the field of AML/CTF, types of ML/TF, implementation of the international sanctions regime.

General risks of the sector

Tax consulting is part of a category of services that criminals (often willing to pay significant amounts) can call upon to try to facilitate criminal activities, conceal the illicit origin of some assets. Consulting services can be used both in the stage of stratification of the ML and in the stage of integration, respectively when trying to carry out some operations/activities through which the funds, after having gone through the laundry process, are invested in various businesses/acquisitions, often in distant geographical areas with different tax legislation.

General risks of the products/services offered in the sector

Regarding the vulnerabilities of tax consulting services, we present by way of example situations in which tax consultants may be requested by criminals (who will thus try to make up for their lack of experience in the financial-fiscal field) to provide services such as:

- consultancy in the sense of documenting the tax regulations and regimes of several jurisdictions, including in offshore centers, where money launderers can establish various companies with "opaque" ownership and control structures (thus facilitating the concealment of the identity of the real beneficiary);
- consultancy so as to avoid the payment of tax, within the limits of the law, directing the money towards a more favorable tax regime, in the context where, applying risk-based know your client measures, the consultant identifies reasonable suspicions regarding the possible involvement of the client in crimes that may generate illicit funds;
- tax consultancy given to high-risk clients (such as publicly exposed persons) or entities with complex structures (where the identification of the real beneficiary is particularly difficult) that may be involved in complex transactions with the aim of integrating amounts of illicit origin, in the real economy.

General vulnerability of specific sector/products regarding exposure to money laundering risk

The vulnerabilities regarding the preventive measures identified within the supervision activities of the sector reside mainly from the finding of non-compliance with the legal provisions, with an emphasis on the following aspects:

- in several situations, the KYC measures applied did not allow the identification of the real beneficiary of the clients and/or were not taken in accordance with the provisions of the Norms regarding the supervision by NOPCML of the way of implementation of international sanctions;
- in several situations the KYC measures were not applied through risk-based circumstantiation, as the appropriate risk indicators were not used for the risk-based assessment from the ML/TF point of view;

[107] Failure to comply with the provisions of art. 6 of the Rules regarding the supervision by NOPCML of the implementation of international sanctions approved by GD 603/2011

- inadequacies regarding the proper training of employees regarding the provisions of the legislation in the field of AML/CTF and practical aspects that can facilitate their recognition of suspicious transactions;
- deficiencies regarding the establishment/completion/updating/reassessment of the anomaly indicators for the recognition of suspicious transactions within the internal procedures.

Specialists in the field could be involved in managing complex transactions that require tax consultancy. The sector is likely to be used by high-risk customers (such as publicly exposed individuals or customers in areas of significant geographic risk).

According to the Supranational Risk Assessment (2019), the services provided by tax consultants are frequently used in money laundering schemes and may be used by OCGs as a way to compensate for their lack of expertise in the field. The level of vulnerabilities related to the services provided by specialists providing tax advice is therefore considered to be significant.

Competence and probity mechanisms (FIT&PROPER), registration/authorization and oversight mechanisms

The NOPCML and the CTC (Chamber of Tax Consultants) supervise and verify tax consultants on how they apply the provisions of the law so as to prevent and control money laundering and terrorist financing.

Exercising tax consultancy activities by natural persons who have not acquired the status of tax consultant according to the legal provisions or who have not become active members of the Chamber of Tax Consultants, as well as by legal persons who have not been authorized by the Chamber of Tax Consultants or who have not have been registered in the Register of tax consultants and tax consultancy companies is a crime.

The tax consulting activity can only be carried out by persons registered in the Register of tax consultants and tax consulting companies in the active persons sections.

In order to carry out the activity of tax consultancy, the companies must be authorized by the Chamber of Tax Consultants.

The members of the Chamber are:

a) persons who have been issued with a professional card and registered in the Register of tax consultants and tax consultancy companies;

b) the companies that obtained the operating authorization issued by the Chamber and registered in the Register of tax consultants and tax consulting companies.

During the Focus Groups, the representatives of the tax consultants highlighted the fact that, in relation to the activity carried out, risks of exposure to the use of services were identified in some money laundering operations related to fictitious transactions and the use of complex structures with international ramifications, including some complex payment schemes between different entities, including foreign entities. The identification and verification of the beneficial owner is highlighted as an aspect that can involve significant difficulties, usually in connection with obtaining information from the Register of beneficial owners and requesting documents from the client.

Types of money laundering and typical cases of money laundering related to the sector and high-risk products / services

USE OF ACCOUNTS HELD IN ROMANIA BY RESIDENT NATURAL PERSONS FOR THE RECYCLING OF AMOUNTS PROVIDED FROM TAX, BUSINESS OR ACCOUNTING CONSULTANCY AND SERVICES PROVIDED BY EXPERT ACCOUNTANTS, CERTIFIED ACCOUNTANTS, CERTIFIED APPRAISERS	
Description	The typology refers to the presence of a group of related resident individuals (all listed as employees of two resident legal entities: an association and a company). The members of the group act using personal accounts opened with resident credit institutions, bank accounts from which they carry out multiple cash withdrawal operations. Two of the resident individuals have the role of coordinating the above-mentioned group. At the same time, the two also act as authorized agents on the accounts of the association and the resident company, arranging the transfer of significant sums of money to the accounts of employees under the heading of 'salaries', the source being funds obtained from public authorities and not used for the purpose for which they had been accessed within the projects (in this case, indications have been identified in relation to the change, without respecting the legal provisions, of the destination of funds obtained or guaranteed from public funds). Individuals in the group, who had received significant amounts of money from the association and the resident company as salaries, withdrew the money in cash. The two resident individuals who coordinated the group obliged the employees to hand over most of the salaries received in the manner described above. After the group coordinators took possession of the money, these funds were deposited in their personal accounts and then transferred externally through under-reporting transactions to purchase luxury goods.
Profile of natural person/legal entity	The association transferring large sums of money to employees' accounts accessed government funds, and the resident legal entity that made most of the payments to the accounts of several individuals with the explanation mentioned above is a professional working in the fields of accounting, financial auditing, tax consulting, business consulting and management.
Indicators (specific typologies)	- external transfers below the reporting limit from the accounts of individuals controlling the partnership and company to personal accounts opened in an offshore jurisdiction; - repeated receipts into the accounts of more than one individual, the payer being the resident association and the payer being the payroll, followed by cash withdrawals made on the same day or in the immediately following days; - information on the misappropriation of public funds by the president of the association, using some of their employees/bank accounts for this purpose; - multiple cash withdrawals.

MECHANISM	• the discrepancy between the amount of wages paid by the association and the company to the employees compared to the wages paid in the respective sector; • using the accounts of individuals to divert money from government funds; • the involvement of a person working in the fields of accounting, financial auditing, tax consulting, business consulting and management.
INSTRUMENTS	• use of cash; • use of bank accounts; • use of external transfers.

Conclusions:

Given that, although there are factors that mitigate the sector's exposure to money laundering risk, such as:

- the sector is well regulated in terms of the legal framework in force applicable to the profession;
- supervision and control regarding the enforcement of the legislation in the field of AML/CTF are ensured by the NOPCML and the CTC, as a self-regulatory body for the reporting entities that they represent and coordinate;
- the existence of fit&proper mechanisms that ensure the maintenance of certain standards regarding access and retention in the profession and that prevent the access to the profession of convicted persons;
- organization by NOPCML of training seminars for professionals in the sector;

however, considering aspects such as:

- the services provided by tax consultants can be used in money laundering schemes and can be used by OCGs as a way to compensate for their lack of experience in the financial field and to use the experience of professionals to identify methods to hide the illicit origin of some assets, concealing the identity of the real beneficiary by establishing companies with "opaque" ownership and control structures, developing complex and complicated financial flows specific to the ML stratification stage, etc.;
- the analysis carried out by the authorities highlighted the fact that tax consultants are among the professionals who have a significant possibility of being used by criminals in money laundering schemes;
- the degree of awareness of the sector regarding the risks of ML/TF still appears to be limited, given the lack of reports of suspicious transactions originating from this sector;
- the identification, within the supervision activities of the sector, of some non-compliance with the legal provisions, with an emphasis on the following aspects: deficiencies regarding the establishment/completion/updating/re-assessment within the internal procedures of anomaly indicators for the recognition of suspicious transactions, KYC measures applied do not allow in all situations the identification, as the case may be, of the real beneficiary of the clients, the risk-based assessment from the point of view of ML/TF was not carried out properly in several cases and deficiencies were found regarding the application of knowledge measures of the clientele by risk-based circumstantiation and the risk indicators used.

It can be concluded that:

The level of vulnerability to money laundering in respect of the sector is considered significant, which has led to the establishment, at national level, of a medium ML risk rating associated with the sector.

No.	Elements	Likelihood Rating (L)	Assessment of consequences (C)	Rating of risk
	risk tied up of Tax consultants	**Low**	**Major**	**Average**
Associated vulnerabilities: **A relatively low level of awareness regarding how to fulfill the obligation to detect suspicious transactions; Certain weaknesses in the enforcement of anti-money laundering and anti-terrorist financing regulations.**				
Associated threat: **Tax advice given to high-risk clients (such as publicly exposed persons) or entities with complex structures (where the identification of the real beneficiary is particularly difficult) that may be involved in complex transactions with the aim of integrating amounts of illicit origin, in the real economy.**				
Event description: **Consultancy so as to avoid payment of tax obligations, within the limits of the law, directing towards a more favorable tax regime, in the context where, applying risk-based KYC measures, the consultant identifies reasonable suspicions regarding the possible involvement of the client in crimes, which may generate illicit funds.**				
Risk description: ***Medium risk*** ***Low probability*** ***Major consequences***				

4.7.6 Persons providing financial, business or accounting consultancy

General description

In accordance with the legal provisions, persons who provide financial, business or accounting consultancy (including entities that actually carry out the activities referred to in art. 5 paragraph (1) letter e) of the Law according to CAEN code 7022) are considered reporting entities[108], which do not have a regulatory body, sectoral supervision and control or an association of professionals in this field.

The enforcement of the provisions of the law in the field of AML/CTF is supervised and controlled, within the scope of the service attributions, by the NOPCML.

The activity of financial, business or accounting consultancy (CAEN code 7022) may include consultancy, guidance or operational assistance for companies and public services in relation to:

- designing accounting methods or procedures, cost accounting programs, budget control procedures;
- consulting and assistance for companies and public services for planning, efficient organization and control, information management, etc.

[108] In accordance with Article 5 paragraph (1) letter (e) of the Law and Article 3 paragraph (1) letter (c) of Regulation no. 37/2021 implementing the provisions of Law 129/2019

According to information provided by the National Trade Register Office (ONRC)[109], there are approximately 38,916 territorially registered entities that declared business and management consulting activities as their main activity, of which: 30,611 legal entities and 8,305 authorized natural persons.

Specific legislation[110] of the incorporation of companies provides that the founders cannot be persons who, according to the law, are incapable or who have been convicted for fraudulent management, abuse of trust, forgery, use of forgery, fraud, embezzlement, perjury, giving or receiving bribes, for the crimes provided by the Law for the prevention and sanctioning of money laundering, as well as for the establishment of measures to prevent and combat the financing of acts of terrorism, with subsequent amendments and additions, for crimes regarding the insolvency procedure.

During the reference period, NOPCML did not receive any STR from persons providing financial, business or accounting consultancy (CAEN code 7022).

In the cases analyzed by the law enforcement authorities, successive financial transfers made on the basis of fictitious consulting contracts, with tax havens as destinations (Cyprus, British Virgin Islands, Bermuda Island, USA-Delaware) were identified.

Also, the cases analyzed by the authorities revealed that among the most used methods of integrating illicit funds into the legal economy are making transfers based on justifications that are not based on real operations, for example: transfers with the justification of asset purchases /services which in fact are fictitious and difficult to prove (for example transfers with the justification of business consultancy, etc.).

The processed questionnaires show that the entities, which were part of the analyzed sample, demonstrate that most of them have elusive general knowledge regarding the field of combating money laundering and terrorist financing, and do not have a thorough knowledge of the legislation that applies in the field.

General risks of the sector

Taking into account the specifics of the activity, professionals who provide management and business consulting, including financial or accounting aspects, can have numerous contacts and relationships both in the public and private sphere, which can be used by criminals in order to initiate financial circuits, the identification of opportunities in the field of investments on the capital market, the purchase of various goods at competitive prices, the establishment of offshore companies in order to disguise the origin of the goods or other operations that allow them to give an appearance of legality to illicit income.

General risks of the products/services offered in the sector

Due to the types of services they can provide to their clients such as designing accounting methods or procedures, cost accounting programs, general accounting consulting, consulting and assistance to companies, they can help OCGs hide their identity and the origin of their money. Thus, the services they provide are targeted by criminal organizations to compensate for their lack of expertise.

[109]For active entities only, the data refer to the period 31.12.2020-20.01.2021 and have a margin of error of 5%.
[110]Article 6 paragraph (2) of Law no. 31/1990 on companies

Risk situations identified for the services offered/clients of the sector of activity represented by the persons providing financial, business or accounting consultancy:

- The provision of services that, in the absence of effective risk identification and assessment, may facilitate the concealment of the true nature or the concealment of the proceeds of crime;
- After analyzing the circumstances of the transactions, there are reasonable grounds to suspect that the assets traded by the client are the results of a criminal activity.
- Sufficient/clear information is not held regarding the source of wealth and the source of funds of clients and real beneficiaries identified as PEP;
- Clients who, under ambiguous conditions, use off-shore/shell companies or legal entities with assets managed in different countries, apparently without reasonable fiscal, business or economic reasons;
- Clients who appear to be acting on the instructions of another person whose identity is wished to remain unknown, or clients unreasonably avoid business meetings involving direct communication;
- Clients with previous convictions for fundraising offences, who instruct professionals to act on their behalf;
- Clients have funds that are obviously and inexplicably disproportionate to the information held by the entity in applying customer due diligence measures;
- Lack of transparency in the transaction;
- Clients insist, without reasonable explanation, that transactions are carried out exclusively or mainly through the use of virtual assets in order to preserve their anonymity;
- Clients offer to pay unusually high levels of fees for services that would not normally involve such a measure.
- The client asks the professional for advice or the implementation of an arrangement that could have the purpose of committing or concealing a crime.
- The client is reluctant to provide all relevant information;
- Situations where the professional assesses an inadequate motivation, especially when the client does not provide pertinent justifications;
- The client requests advice on creating arrangements that can be used to hide the real beneficiary;
- Services where the professional acts as a proxy and allows the client's identity to remain secondary;
- The professional identifies fraudulent transactions that are improperly accounted for: over/under billing of goods and services, multiple billing for the same goods, falsely described products/services.

The overall vulnerability of the sector and specific products to the risk of money laundering

The experience of professionals in areas such as providing consultancy, as well as their thorough knowledge of the business environment can be extremely useful to money launderers.

Likewise, professionals who provide management and business consultancy, including financial or accounting aspects, can be used as a means of creating structures for the movement of illicit funds.

Therefore, the money laundering threat level related to financial, business or accounting consultancy services is considered to be high.

Types of money laundering and typical cases of money laundering related to the sector and high-risk products / services

Description of risk events

a) The transfer of the sums obtained from the crime of tax evasion outside the country, disguised in the form of a commission-consultancy contract. In the case, a criminal group was investigated that led and supervised withdrawals from banking units of large amounts of cash obtained from the sale of fuel without payment of excise duties to the state. The illegal proceeds were laundered by one of the defendants and the legal entity of which he was an administrator, through the bank accounts held by the companies controlled by the coordinator of the group in Dubai, United Arab Emirates. They transferred, through repeated transactions, the total amount of 13,212,000 dollars of the sums obtained from tax evasion to an account in Dubai controlled by the group coordinator, registering fictitious consulting operations as justification, in order to disguise the origin.

Conclusions: Among the specific elements of the operation mode of the OCG in Romania is the use, in successive transactions, of fictitious financial consultancy contracts.

Conclusion:

In Romania, the entities within the sector are not coordinated by a self-regulatory body.

The cases analyzed by the authorities revealed that among the most used methods of integrating illicit funds into the legal economy are transfers based on justifications that are not based on real operations, for example transfers with the justification of business consultancy.

Services provided by professionals providing managerial and business consultancy, including financial or accounting, can be frequently used in ML schemes and are considered by criminals to be the best way to compensate for their lack of expertise. Therefore, the level of money laundering threat related to services provided by persons providing financial, business or accounting advice is considered high.

Risk mitigating factors in the sector:

The supervision and control of the way of applying the legislation in the field of AML/CTF by this category of reporting entities is ensured by NOPCML, which regularly organizes training sessions dedicated to this sector;

No.	Elements	Likelihood Rating (L)	Assessment of consequences (C)	Risk rating
	Risk related to persons providing financial, business or accounting advice	**Average**	**Major**	**High**
Associated vulnerabilities: **The lack of transparency of transactions that can facilitate the concealment of the true nature or the concealment of the proceeds of crime;** **The degree of awareness of the sector regarding the risks of ML/TF still seems to be limited considering the lack of reports of suspicious transactions originating from this sector;**				

Associated threat: **Because of the types of services they can offer their clients, they can help OCGs hide their identity and the origin of their money.**
Event description: **Providing services which, in the absence of effective customer identification and risk assessment of the types of transactions requested by customers, may facilitate the concealment of the true nature or concealment of the proceeds of crime.** **The client may ask the professional for advice or the implementation of an arrangement that could have the purpose of committing or concealing a crime.**
Risk description: ***High risk*** ***Average probability*** ***Major consequences***

4.7.7 Public notaries

General description

Public notaries are regulated as reporting entities and fall under the provisions of Law no. 129/2019, article 5, paragraph (1) letter (f).

According to the Law of notaries public and notarial activity no. 36/1995, republished, with subsequent amendments and additions, the forms of exercising the function of public notary are: individual office and professional association. Notaries public associated in a professional association exercise their duty in person and are individually liable for their activity.
The public notary cannot exercise his function, at the same time, in several forms of exercising it.

In the analyzed cases, a situation was identified in which a notary public authenticated several successive sale contracts (with the same property-land as object) within unusually short time intervals, there being suspicions that were not reported.

Another case reviewed was in relation to the establishment of an organized criminal group to obtain money from human trafficking and to loan the money at interest rates that often exceeded the value of the loan. Thus, in order to hide the illicit origin of the funds involved in the transactions, part of the money from human trafficking was lent to third parties at very high interest rates, in the context in which fictitious loan contracts with real estate guarantees were authenticated at several notary offices.

According to the analysis carried out by the authorities, there were situations in which notaries public did not submit STRs related to the repeated nature of loans offered by the same person, the unusually large total sums involved in the transactions, the legal nature of the contracts (usually loan with mortgage); there is even a suspicion of complicity with the persons involved in the criminal activity.

According to the analysis carried out in the assessment, public notaries are among the professions most exposed to the risks of using the services offered for money laundering operations. At the same time, in the vast majority of money laundering schemes, intermediaries and influential persons with important public positions were used so as to

facilitate transactions with money from crimes. Public notaries can be a vulnerable link in the networks used in complex and complicated schemes whose objective is to conceal the true nature of some funds.

In 2018, notaries public sent to NOPCML a number of 1,090 STRs, in 2019 they sent a number of 1,191 STRs, and in 2020 they sent a number of 762 STRs.

Regarding the results of the off-site and on-site surveillance activity (compliance checks) carried out during the reference period by NOPCML in relation to the "notaries public" sector, we mention the following:

- off-site surveillance: 98 entities (2019); following the off-site supervision, carried out according to NOPCML's internal procedure for the supervision of reporting entities, during the reference period, for the "public notaries" sector, 26.6% of the supervised entities were classified as having a high degree of risk and 14.3% were classified as having a partially high degree of risk;
- on-site supervision: 16 entities (2019) with 3 sanctions applied (2019: 2 warnings and 1 fine of 15,000 lei) for violations regarding: art.11 of Law 656/2002, GD 603/2011, art.5(7) of Law 656 /2002.

According to the provisions of art. 160 of the Law regarding public notaries and notarial activity, namely Law 36/1995, with subsequent amendments and additions, combined with the provisions of art. 85 para. (l) from the law enforcement regulation, the National Union of Notaries Public in Romania (hereinafter referred to as UNNPR) exercises professional administrative control through the Union's Control Body, which carried out specific controls during the reference period, some notaries public being verified. One of the objectives of the UNNPR controls was the compliance with the provisions of the law for the prevention and control of money laundering and the financing of acts of terrorism, and the control teams found that, as a rule, the obligations to report cash and suspicious transactions were fulfilled, such as and the fact that, as a rule, notaries draw up the customer information sheet.

Also, the Union Council can delegate the exercise of professional administrative control to the Boards of Directors of the Chambers of Public Notaries. In the period 2018-2020, the Chambers of Public Notaries carried out professional administrative control at various notary offices, and in some situations, among the objectives of the control was the verification of compliance with the provisions of the law for the prevention and combating of money laundering and the financing of acts of terrorism.

From the processed questionnaires, it emerged that most of the entities that were part of the analyzed sample have elusive general knowledge regarding the field of combating money laundering and terrorist financing, and do not have a thorough knowledge of the legislation that applies in the reference field.

General risks of the sector:

It is necessary for public notaries to pay particular attention to the fulfillment of their duties according to the provisions of the legislation on the prevention and control of ML/TF, analyzing every time, in the case of potentially suspicious transactions, all the circumstances, data and information that determine the extent to which reporting is necessary. Training but

also individual training in this matter are extremely important, being very useful the frequent consultation of the NOPCML website, where several guides/manuals/legislation/useful typologies have been published, and also the participation of public notaries in the training sessions organized by NOPCML in collaboration with UNNPR.

Public notaries perform a significant number of support services for clients involved in various financial transactions, for example various aspects that may be related to their organization and/or management. Public notaries could be directly involved in situations related to the conduct of financial transactions of various types, for example various procedures in connection with keeping some funds or paying the price of some real estate. However, all these perfectly legitimate attributions can be used by OCGs/criminals, who in some cases may try to take advantage of the experience of such professionals, with the aim of creating schemes that help launder the proceeds of crime[111].

General risks of the products/services offered by the sector:

Public notaries, in the course of their work, may come into contact with criminals and/or receive important information regarding businesses that hide illicit purposes such as money laundering.

The analyzes carried out highlight the fact that real estate is frequently used in ML schemes and since within such schemes the services of notaries public can be combined with those provided by other professionals in the non-financial sector, the level of exposure to ML risk related to transactions with real estate is considered high. Therefore, public notaries, within the activities related to transactions in the real estate sector, can reduce vulnerability to the risk of ML/TF by properly fulfilling all their obligations under the law to prevent and combat money laundering and terrorist financing.

Regarding the types of products/services provided within the sector, assessed as being exposed to risk from the point of view of money laundering and terrorist financing, the following products/services present general risks regarding exposure to the phenomenon of money laundering:

1. Contracts for sale - purchase of real estate;
2. Contracts for sale - purchase of movable goods;
3. Exchange contracts;
4. Loan contracts;
5. Warranty contracts;
6. Contracts of donation of movable property;
7. Real estate donation contracts;
8. Receivables assignment contracts;
9. Trust contracts;
10. Bailment contracts;
11. Certificates of inheritance;
12. Dated documents/statements;
13. Payment documents;
14. Shares;
15. Legalization of signature of the parties;
16. Other types of notarial acts.

[111] http://www.onpcsb.ro/pdf/MANUAL%20INSTRUIRE%20-%20ROMANA.pdf.

General vulnerability of the sector / specific products to the risk of money laundering

During the on-site supervision, the control teams mainly made the following recommendations to remedy some deficiencies/optimize the AML/CTF activity:

- compliance with all legal provisions, including how to implement international sanctions, keeping proof of client inquiry/verification using the information available on the NOPCML website - international sanctions section (recommendation for most verified entities);
- periodically checking the NOPCML website www.onpcsb.ro to identify possible legislative changes/news in the specific field as well as courses/trainings organized by NOPCML, guides, manuals published on the site (recommendation for most verified entities);
- compliance with all legal provisions in the field of applying KYC measures, including the correct identification of the real beneficiary;
- classifying customers according to the associated ML/TF risk in order to be able to correctly identify the cases in which additional customer due diligence measures are applied, as well as the appropriate establishment of these measures;
- drafting/updating/completion (as appropriate) of policies and procedures that contain ways to identify the real beneficiary, anomaly indicators, risk indicators, application of measures to know the clientele through risk-based circumstantiation, respectively drawing up internal documents that demonstrate the implementation of these procedures;
- employee training; designation of a person with responsibilities in the enforcement of
- the law for the prevention and control of money laundering and the financing of terrorism;
- establishing anomaly indicators - identifying suspicious transactions.

In order to distance criminal activity as far as possible from the actual movement of the resulting funds, criminal groups could use the services of third parties, including professionals such as public notaries. A FATF guide indicates that criminals often seek the involvement of legal professionals in money laundering or terrorist financing activities, as these professionals may be asked to identify the best way to complete certain transactions or to use specialized legal/notary services, both of which can contribute to the laundering of the proceeds of crime.

Fit&proper mechanisms, registration/authorization and surveillance mechanisms:

In Romania, public notaries are appointed by the Minister of Justice, upon the proposal of the Union Council, based on the request of the interested party and after proving the fulfillment of the conditions stipulated by the Law on public notaries and notarial activity no. 36/1995, republished with subsequent changes.

The National Union of Notaries Public in Romania (UNNPR) is the only professional organization of notaries public in Romania.

All notaries public in Romania are members of the UNNPR and are organized, at the territorial level, in 15 Chambers of Public Notaries that operate within the jurisdiction of the Courts of Appeal. The basic structural element is the office of the notary public, and the

notary activity is carried out by notaries public through notarial documents and notarial legal consultations under the conditions of the law[112].

According to the provisions of art. 22 paragraph (l) letter d) of Law no. 36 of May 12, 1995 (republished), a notary public must have no criminal record resulting from the commission of a service crime or in connection with the service or the intentional commission of another crime.

According to the legislation in force, the capacity of notary public ceases when a final court decision has ordered the conviction or the postponement of the application of the penalty for the commission of an official crime or in connection with the service or for the intentional commission of another crime[113].

Thus, persons definitively convicted for the crime of money laundering or terrorist financing cannot acquire the status of notary public, and if this conviction occurs during the period in which the person already held the status of notary public, the final conviction entails the termination of the status of notary public, ordered by order of the Minister of Justice. Regarding the "fit&proper test", in addition to a clean criminal record when registering or starting an activity, the self-regulatory body has established certain mechanisms to ensure the maintenance of certain standards within the profession. Thus, in case of a conviction of the public notary, the court directly communicates the final decision to the notary chamber, and the appropriate measures will be taken.

According to UNNPR[114], within the meaning of Law no. 129/2019, the real beneficiaries of notary offices are public notaries in all situations.

Notaries public and real estate agents have highlighted various challenges related to the implementation of the obligations arising from the provisions of the legislation on the prevention and combating of money laundering and the financing of terrorism, including regarding the identification and verification of information regarding the real beneficiary of the clients, the source of the funds involved in transactions and source of wealth.

Regarding the verification of the source of funds/wealth, the measures applied are mainly based on the self-declaration of the customers. No other documents/information are required to verify the source of funds/assets.

Notaries regularly participate in the training sessions dedicated to the prevention and combating of money laundering and terrorist financing organized by NOPCML in collaboration with UNNPR and are usually aware of the obligations they have according to the legislation in the reference field, the aspects regarding customer awareness measures and the requirements in reporting matters.

Public notaries have confirmed the real estate sector's high vulnerability to exposure to money laundering, particularly due to difficulties in verifying the source of funds and identifying and verifying beneficial ownership information for clients. The use in the real estate and construction sector of non-resident legal entities, especially those in off-shore areas, was identified as a predominant typology.

---

[112]http://www.uniuneanotarilor.ro

[113]Law no. 36 of May 12, 1995 (*republished*) to public notaries and notarial activity art. 41 paragraph 1 letter f

[114] UNNPR reply no.7832/26.11.2021

Conclusions:

In the course of their work, public notaries might come into contact with criminals and/or become aware of important information regarding economic activities aimed at money laundering, i.e. hiding funds of illicit origin.

In conclusion, there are factors that mitigate the sector's exposure to money laundering risk, such as:

- the fact that public notaries are well organized in terms of the legal framework applicable to the profession, the attributions and role of the UNNPR, the diligence that notaries perform when carrying out their activity, are factors that reduce the level of vulnerability within the sector;
- the supervision and control of the way of applying the legislation in the field of AML/CTF are ensured by NOPCML and by UNNPR, as a self-regulatory body for the reporting entities that they represent and coordinate;
- the existence of fit&proper mechanisms that ensure the maintenance of certain standards regarding access and retention in the profession and that prevent the access to the profession of convicted persons;
- organization by NOPCML of training seminars for professionals in the sector.

Considering aspects such as:

- the exposure risk of some of the services and products offered by public notaries;
- the modest quality of some of the suspicious transaction reports submitted by entities in this sector due to the lack of relevant information;
- the finding, during the compliance control actions carried out by NOPCML, of some deficiencies regarding: the identification of the real beneficiary of the clients, the classification of clients according to the ML/TF risk associated with them and the controlled entities have not established, in all cases, complete internal procedures and complex, applicable in the various stages of their current activities, in order to minimize the vulnerability to the phenomena of money laundering or terrorist financing;

have determined the establishment of an average degree of risk of exposure to ML associated with the notary public sector.

No.	Elements	Likelihood Rating (L)	Assessment of consequences (C)	Risk rating
	The risk in the field of public notaries	**Low**	**Major**	**Average**
Associated vulnerabilities: **The services provided are complex and include a wide range of activities that may be requested by criminal groups that would benefit from the experience/specialization of public notaries.** **The use of cash by clients, in the context of which the law for the strengthening of financial discipline sets a ceiling for such operations, which mitigates the risk.**				
Associated threat: **Using complex notary services to hide the illicit provenance of some assets.**				
Event description: **Authenticating loan contracts to disguise usury.** **Authentication of real estate sales-purchase contracts, the respective real estate transactions constituting links in money laundering schemes**				
Risk description:				

Medium Risk Low Probability Major Consequences

4.7.8 Lawyers

General description

Lawyers are regulated as reporting entities and fall under Law 129/2019 according to art. 5 paragraph (1) letter f., if they provide assistance for the preparation or completion of operations for their clients and if they participate on behalf of or for their clients in any operation of a financial nature or concerning immovable property, or the creation, operation or administration of trusts, companies, foundations or similar structures. Supervision and control of the enforcement of AML/CTF legislation is ensured by the NOPCML and the National Union of Bar Associations (hereinafter referred to as UNBR).

Lawyers carry out a free and independent activity with autonomous organization, operation and management, established under the conditions provided by Law no. 51/1995 for the organization and exercise of the lawyer profession, republished, with subsequent amendments and additions. All bar associations in Romania are legal members of the National Union of Bar Associations in Romania (UNBR). The bar is made up of all the lawyers registered in the list of lawyers who have their main professional headquarters in the localities within its radius. The establishment of bars outside the UNBR is prohibited.

According to the data published on www.unbr.ro, there are 42 bar associations, legally established and operational, out of which 41 bar associations operate in the counties and one bar association in Bucharest. In Romania, more than 30,000 lawyers are enrolled in the Bar; 23,394 lawyers have the right to practice the profession; among them, 19,005 are active lawyers. Among the active lawyers, 952 are legal entities (professional civil companies - 839 and professional limited liability companies - 114) and 18,052 are authorized natural persons who carry out their activity in individual offices.

Analyses carried out by NOPCML have showed that in the period 2018-2020, there was one case involving a lawyer who was referred to law enforcement authorities. The predicate offense found was abuse of office, the amount involved was EUR 1,000,000, and the activity sector in which the offense was committed was pharmaceutical, the subjects being resident natural persons.

Regarding the submission of STRs, between 2018-2020, lawyers submitted only 7 STRs, a small number compared to the size of the sector, indicating a potentially low level of awareness of the ML/TF risks related to the sector.

According to the law enforcement authorities, one of the vulnerabilities identified in relation to the activity carried out by lawyers consists in the fact that legitimate legal services can be used by interested persons in order to hide the real purpose for which the trust contracts are concluded, the trust account can be used to collect illicit money and transfer it to members of the criminal group. A similar situation can also be encountered in the case of the provision of

legitimate legal services for the establishment of commercial companies that could later be used by the interested parties to hide the illicit origin of the money.

The possibility of lawyers to establish, with increased frequency and without a specific regulation focused on AML/CTF issues, companies with registered office established at a lawyer's office, without an office where economic activity can be carried out, was considered also a vulnerability.

At the same time, law enforcement authorities draw attention to the fact that, under the pretext of obtaining legitimate legal advice, interested persons can also obtain from the lawyer information that can be used for the purpose of circumventing the legal provisions regarding the prevention and combating of money laundering.

The exposure to the risk of being used in ML operations concerns in particular those categories of lawyers/law firms with experience in setting up and managing companies in off-shore areas as well as lawyers who have connections with different jurisdictions where their clients request the establishment of companies or lawyers who are required to open bank accounts in jurisdictions other than those of the state of residence of the established companies.

In the period 2018-2020, NOPCML supervised off-site, by introducing in the framework of an analytical process that includes a risk assessment matrix that reveals the degree of exposure to the risk of money laundering and terrorist financing of the reporting entity, a number of 144 entities from the sector represented by lawyers, 15.2% of which are classified as high ML risk.

In the same reference period, NOPCML supervised on-site (on-site inspections) a number of 49 entities in the sector represented by lawyers. As a result of the on-site control actions carried out by NOPCML, a series of violations of the legal provisions in the field of AML/CTF were identified, as a result, the control teams trained the legal representatives of the verified entities on the optimal methods of compliance with the framework legally in the matter, with appropriate contravention sanctions being applied and at the same time with recommendations for remedying the violations found regarding:

- failure to apply KYC measures regarding the implementation of international sanctions, i.e. accessing the consolidated lists of international sanctions and keeping a proof of query/verification on the website - "International Sanctions" section;
- failure to comply with all legal provisions in the field of customer due diligence, including the correct identification of the real beneficiary;
- non-elaboration/non-completion/non-updating of internal procedures/documents adapted to the activity carried out regarding the application of knowledge measures of the clientele through risk-based circumstantiation, risk indicators, real beneficiary identification, the way of applying KYC measures regarding the way of implementing international sanctions;
- employee training;

Anti-money laundering training

During the reference period, NOPCML organized 5 training sessions for the sector represented by lawyers, the subject of the training aimed at practical aspects regarding the application of legal provisions in the field of AML/CTF, types of ML/TF and the implementation of the international sanctions regime.

From the surveillance carried out, in accordance with the National Risk Assessment (NRA) methodology, it emerged that the entities that were part of the analyzed sample demonstrate that most of them have an elusive general knowledge in the field of combating money laundering and terrorist financing and do not have in-depth knowledge with regarding the applicable legislation in this field, but a constant interest from lawyers in order to know the rules in the field of AML/CTF was found.

General risks of the sector:

Organized crime groups often use shell companies ("PO" companies) to carry out complex money laundering schemes. They can also use the services of a lawyer who can provide a full range of services, including setting up companies and facilitating the opening of new bank accounts[115], with the aim of creating the necessary framework for the ML/TF process.

The expertise of legal professionals could be targeted by criminal organizations, including both advising on the best types of offshore companies or locations that could be used in money laundering or terrorist financing schemes, and setting up by companies or management companies in order to use the various opportunities offered by other jurisdictions and the financial system for the purpose of money laundering or terrorist financing. Professionals can also be used to give the appearance of legality to transactions by providing brokerage services in dealings with financial institutions[116].

General risks of the products/services offered in this sector:

First of all, lawyers can advise individuals and legal entities in areas such as: investments, establishment of companies, administration and other legal arrangements, as well as regarding the optimization of the fiscal situation. In addition, lawyers prepare and, if necessary, collect the necessary documentation for the establishment of companies and other legal constructions[117]. This type of legitimate services provided by lawyers can be extremely helpful to money launderers in order to conclude some contracts that legitimize the running of operations aimed at recycling some funds, running some more sophisticated financial circuits and establishing some off-shore companies in order to disguise the origin of the goods, all of which can be used for the purpose of creating an appearance of legality for illicit income.

According to information provided by law enforcement authorities, legal professionals may be used in money laundering schemes.

Competence and integrity mechanisms – fit&proper, registration/authorization and oversight mechanisms:

The profession of lawyer is organized and practiced on the basis of a legal framework[118] well defined, in relation to which, the professional title of lawyer is acquired and valued, by public order rules, because the organization and exercise of the profession of lawyer does not belong

---

[115] *(https://www.fatf-gafi.org/media/fatf/documents/Professional-Money-Laundering.pdf-GAFI (2018), Professional Money Laundering, GAFI, Paris, France)*

[116](http://www.onpcsb.ro/pdf/MANUAL%20INSTRUIRE%20-%20ROMANA.pdf)

[117] *(http://www.onpcsb.ro/pdf/MANUAL%20 instruct% 20-% 20 Romania.pdf)*

[118]Law no. 51/1995, with subsequent amendments

to the private domain, and the professional title of lawyer cannot be acquired or assigned outside of this legal framework, mandatory for all public authorities, including courts.

The profession of lawyer is practiced only by lawyers registered in the bar where they belong, part of the National Union of Bar Associations (UNBR)[119]. The establishment and operation of bar associations outside the National Union of Bar Associations in Romania is prohibited, and their establishment and registration documents are null and void[120].

Regarding the fit&proper conditions, to enter the legal profession, in addition to the criminal record that does not result in a state of indignity, according to the law required when registering or starting to practice, the self-regulatory body (UNBR) emphasized that the legislation in force provides mechanisms to ensure the maintenance of certain standards of access and retention in the profession. Thus, according to art. 14 lit. a) from Law 51/1995, he is unworthy to be a lawyer, who is definitively sentenced by a court decision to prison for committing an intentional crime likely to harm the prestige of the lawyer profession, to which are added the decisions of the Constitutional Court of Romania pronounced with regard to art. 14 lit. a) from Law 51/1995.

Note:
*By Decision of the Constitutional Court no. **225 of April 4, 2017**, published in the Official Gazette of Romania, Part I, no. 468 of June 22, 2017, the exception of unconstitutionality was admitted, finding that the phrase "likely to harm the prestige of the profession" is unconstitutional.*
*By Decision of the Constitutional Court no. **230 of April 28, 2022**, published in the Official Gazette of Romania, Part I, no. 519 of May 26, 2022, the exception of unconstitutionality was admitted, finding that the provisions of art. 14 lit. a) from Law no. 51/1995 for the organization and exercise of the lawyer profession are unconstitutional.*

Also, the capacity as a lawyer ceases[121] if the measure of expelling from the profession was taken against the lawyer as a disciplinary sanction, according to the law.

During the discussion in the focus groups gathered for this risk assessment, the representatives of the lawyers emphasized the following aspects regarding the impact of the obligations regarding the fight against money laundering and the financing of terrorism on the activity of the lawyers:

- the issue of professional secrecy i.e. situations where lawyers are not obliged to submit an STR when considering information they receive from or obtain in relation to their clients in the course of: assessing the client's legal position in legal proceedings, representing the client in or in connection with legal proceedings, giving legal advice on the initiation or avoidance of legal proceedings. By exception, as provided for in the current legal framework, it has been emphasized that lawyers are obliged to submit a STR in cases where they know that legal advice is provided for the purpose of money laundering or terrorist financing or they know that a client wants legal advice for the purpose of money laundering or terrorist financing, subject to the provisions of Art. 33 para. (5) of Law 129/2019.

[119]Art. 1 paragraph (2) from Law no. 51/1995, with subsequent amendments
[120]Art. 1 paragraph (3) from Law no. 51/1995, with subsequent amendments
[121]according to Law no. 51 of June 7, 1995 (*republished*) for the organization and exercise of the profession of lawyer - art. 26 paragraph 1 lit. c) and letter d)

- highlighted two major risks of exposure to the phenomenon of money laundering faced by the profession, namely the situation in which lawyers host the registered office of some companies and the situation in which lawyers provide services for trusts or similar legal constructions
- The Council of the UNBR established a working group to analyze the impact of the obligations regarding the fight against money laundering and the financing of terrorism on the activity of lawyers and the respect of professional secrecy of the lawyer, the issue of risk-based supervision of the sector in terms of combating money laundering and terrorist financing posing a challenge for UNBR.

- there is a constant improvement in the level of understanding and knowledge among lawyers regarding their AML/CTF obligations, in particular the suspicious transaction reporting obligations under AML/CTF legislation but also especially regarding professional secrecy.

Types of money laundering and typical cases of money laundering related to the sector and high-risk products / services

USE OF ACCOUNTS HELD IN ROMANIA BY RESIDENT LEGAL PERSONS ESTABLISHED AT THE HEADQUARTERS OF A LAW OFFICE FOR THE RECYCLING OF AMOUNTS PROCEEDED FROM COMPUTER FRAUD	
Description	The typology is characterized by the presence of a group of resident legal entities established by non-resident natural persons (with the same nationality). Legal entities have the same transaction pattern. Resident legal entities have collected significant sums of money from non-resident natural and legal entities through their bank accounts. The funds collected in this way were transferred to the account of legal entities in Asian countries, via internet banking. Resident legal entities were established in order to defraud highly confidential IT systems by stealing the identity of senior management (cloning email addresses) who had the right to make decisions about making transactions/investments of securities substantial.
Profile of natural person/legal entity	Group of resident legal persons established by non-resident natural persons (with the same nationality) in a relational relationship, all appearing with their registered office at the same address, in this case a law firm.
Indicators (type-specific)	- accounts inactive for a long period of time, activated by a high-value external collection; - immediate transfers of collected amounts to jurisdictions in the Asian area; - using the accounts of resident legal entities as transit accounts; - - information received from the correspondent bank regarding a possible fraud; the inconsistency between the justifications of the transactions carried out and the main object of activity declared by the resident legal entities.
MECHANISM	• the use of the accounts of legal entities in order to remove the criminal proceeds from the illicit source and the transfer of these amounts to areas where they can be traced with difficulty; using Internet banking in order to make transactions as quickly as possible, so that the sums of money cannot be blocked;
INSTRUMENT	-use of bank accounts; -use of external transfers.

Conclusions:

Given that, although there are factors that mitigate the sector's exposure to money laundering risk, such as:

- the fact that the sector is well regulated in terms of the legal framework in force applicable to the profession;
- the supervision and control of the way of applying the legislation in the field of AML/CTF are ensured by NOPCML and by UNBR, as a self-regulatory body for the reporting entities that they represent and coordinate;
- the existence of fit&proper mechanisms that ensure the maintenance of certain standards regarding access and retention in the profession;
- organization by NOPCML of training seminars for professionals in the sector;

However, considering aspects such as:

- some of the services and products that lawyers offer may be attractive to money launderers;
- the activity of lawyers can be used contrary to the purpose of the profession when they are asked to establish off-shore companies, which are used to hide the illicit circulation of some funds;
- criminals are often tempted to resort to the specialization of lawyers, whose professional secrecy is protected by law, which could lead to the refusal of professionals in the sector to disclose information related to the client;
- the degree of awareness of the sector regarding the risks of ML/TF still appears to be limited given the low level of reporting of suspicious transactions;
- the identification, during the control actions carried out by the NOPCML, of the fact that, in the case of individual clients, verifications are not always carried out or evidence of the check on the international sanctions lists is not kept, the identification of the real beneficiary of the clients is not always carried out and there is, at the level of all entities, a classification of clients according to the associated ML/TF risk;
- the existence of deficiencies in the way this category of professionals performs checks and manages risks;
- the controlled entities have not implemented complete and complex internal procedures to regulate the activity in such a way as to minimize the vulnerability to the phenomenon of ML/TF.

the level of vulnerability to money laundering in relation to legal advice provided by lawyers is considered significant, which led to the establishment, at national level, of a medium ML risk associated with the lawyers sector.

No.	Elements	Likelihood Rating (L)	Assessment of consequences (C)	Risk rating
	The risk in the field of lawyers	**Low**	**major**	**average**

Associated vulnerabilities: **The activity of lawyers can be used by persons of bad faith, contrary to the purpose of the profession, when they are asked to establish companies that are later used to hide the illicit origin of some funds, including the establishment of off-shore companies.** **Abusive invocation of the confidentiality clause by lawyers, which could lead to the situation where some of the professionals would consider that they have reasons to avoid reporting suspicious transactions.** **The possibility of setting up with increased frequency and without a specific regulation focused on AML/CTF issues, companies with registered offices at a law firm, under conditions that raise suspicions.**
Associated threat: **Lawyers' thorough knowledge of the business environment can be extremely useful for money launderers to contact various professionals in order to obtain, with the appearance of legitimacy, information to facilitate the laundering of proceeds of crime.**
Event description:
Establishing the main offices of companies at a lawyer's office by clients who intend to disguise the true nature of the company's business or hide the identity of the real beneficiary.
Risk description: ***Medium risk*** ***Low probability*** ***Major consequences***

4.7.9 Bailiffs, insolvency practitioners, other persons exercising liberal legal professions

General description

Bailiffs, insolvency practitioners and other persons practicing liberal legal professions are regulated as reporting entities and fall under the scope of Law 129/2019 according to art. 5 paragraph (1) letter f., if they provide assistance for the preparation or perfecting of operations for their clients and if they participate on behalf of or for their clients in any operation of a financial nature or regarding real estate, or in the creation, operation or administration of trusts, companies, foundations or similar structures.

The supervision and control of the way of applying the legislation in the field of AML/CTF, for bailiffs, is ensured by NOPCML and by the National Union of Bailiffs (hereinafter referred to as UNEJ) - as a self-regulatory body for the reporting entities that they represent and coordinate, and for insolvency practitioners by NOPCML and the National Union of Insolvency Practitioners in Romania (hereinafter referred to as UNPIR) - as a self-regulatory body for the reporting entities it represents and coordinates.

(a) ***Bailiffs*** are organized in accordance with Law no. 188/2000, republished, with subsequent amendments and additions, according to which bailiffs are invested to provide a service of public interest, and the coordination and control of their activity is exercised by the Ministry of Justice. The bailiff is appointed by the minister of justice in the jurisdiction of a court and is registered in the List of Bailiffs (in which 757 bailiffs are registered). Bailiffs are members of the National Union of Bailiffs (UNEJ).

According to art. 7 para. (1) from Law no. 188/2000, bailiffs have, among others, the enforcement of the civil provisions of the enforceable titles and the amicable recovery of a claim.

The members of the National Union of Bailiffs are all bailiffs working in Romania, appointed by the Minister of Justice. The National Union of Bailiffs, the UNEJ, manages and coordinates the work of bailiffs nationwide and monitors compliance with the rules of

professional conduct in their field, in accordance with the Code of Professional Conduct. The conviction at first instance of a bailiff leads to his or her suspension from his or her post, and his or her status as a bailiff ceases when the court decision ordering the conviction or the postponement of the enforcement of the sentence against the bailiff becomes final. Furthermore, any judgment convicting or confirming the disciplinary penalty imposed is brought to the attention of the UNEJ ex officio by the courts.

Regarding the application of the provisions of Law no. 129/2019, the National Union of Bailiffs (UNEJ) as a self-regulatory body developed the Procedure in the matter of preventing and combating money laundering, which was communicated to all its members. In partnership with NOPCML, it organized the professional training of bailiffs, in order to increase the level of knowledge of the legislation in the field.

(b) ***Insolvency practitioners*** are organized by GEO no. 86/2006 on the organization of the activity of insolvency practitioners, republished, with subsequent amendments and additions. Insolvency practitioners are members of the National Union of Insolvency Practitioners in Romania (UNPIR).

Regarding the types of products/services provided, in accordance with the provisions of art. 1 of GEO no. 86/2006, UNPIR members conduct insolvency and voluntary liquidation procedures, insolvency prevention procedures, financial supervision or special administration measures.

Insolvency practitioners can have the capacity of judicial administrators, liquidators, conciliators, as well as any other capacity provided by law. Depending on the quality they have, they:

- exercise the powers provided by law or established by the court, in the insolvency procedure, during the observation period and during the reorganization procedure (judicial administrator);
- manage the debtor's activity within the bankruptcy procedure, and exercises the powers provided by law or those established by the court (judicial liquidator);
- exercise the powers provided by law or those established by the syndic judge, within the preventive arrangement procedure (the arrangement administrator);
- exercise the powers provided by law within the restructuring agreement (restructuring administrator).

Insolvency practitioners can practice their profession in individual firms, associated firms, professional limited liability companies (SPRL) and sole proprietorships with limited liability or they can have the capacity of collaborators or employees of one of the forms of practicing the profession.

UNPIR was the first professional organization in Romania that included in its operating law the right to free practice of persons holding the same professional qualification in the member states of the European Union or belonging to the European Economic Area, the respective provisions being in accordance with the directives of the European Union, regarding to the free movement of people, services, goods and capital.

When entering the activity/profession, persons in a state of indignity (understanding by this including persons who have been definitively convicted of money laundering or terrorist financing crimes) are not accepted in order to acquire the qualification of insolvency

practitioner. Furthermore, if an insolvency practitioner is found guilty of such an offence, the penalty is expelling from the profession.

Regarding the application of the provisions of Law no. 129/2019, the National Union of Insolvency Practitioners in Romania initiated the transposition of the legal provisions through secondary regulations, which aimed to:

- the organization of online or in-room seminars, or the promotion of events organized by UNPIR's external partners, in which information was disseminated regarding the application of the provisions of Law no. 129/2019 from the perspective of practicing the profession of insolvency practitioner;
- informing insolvency practitioners about their obligations as a reporting entity from the perspective of applying the provisions of Law no. 129/2019, by making internal communications or posting on the website www.unpir.ro.

(c) Other persons exercising liberal legal professions and carrying out legal activities: a number of 230 persons are registered with ONRC, of which: 226 legal persons and 4 authorized natural persons carrying out independent activities.

During the reference period, at the NOPCML level, the sectors "bailiffs", "insolvency practitioners" and "other persons exercising liberal legal professions" were not subject to off-site/on-site supervision.

Regarding the "fit&proper test" to enter the profession, when registering or starting to practice the profession, the self-regulatory body in addition to a clean criminal record, representatives of these liberal professions pointed out that there are mechanisms to ensure the maintenance of certain standards regarding access and retention in the profession.

Risks/Threats:

The expertise of bailiffs and insolvency practitioners, as legal professionals, as well as their thorough knowledge of the business environment could be extremely useful to money launderers in order to carry out more sophisticated/complex transactions and conclude contracts that legitimize the running of operations that could aim to recycle some funds.

At the same time, due to the specific nature of the activity, bailiffs and insolvency practitioners have numerous contacts and relationships both in the public and private spheres, reasons why criminals could be tempted to resort to these legal professionals to identify opportunities in the field of investments on the capital market, for the initiation of financial circuits and the like, all of which can be used for the purpose of creating an appearance of legality for illicit income.

During the procedures related to the verification of the debtor's solvency, verification of the debtor's availability, verification of his assets and payment capacities, bailiffs may face atypical, unusual circumstances regarding activities such as the purchase and sale of undervalued or overvalued real estate, any client (creditor) transactions involving the transfer of significant sums of money, securities (e.g. shares and bonds) or other assets whose value is significant.

Insolvency practitioners may also be at risk of being used in money laundering operations, at stages that take place outside of insolvency proceedings and when assisting in the sale of

assets from the company's patrimony, when administering bank accounts, financial instruments, securities or other goods, conclude financial operations and sales of goods, shares or social parts or elements of the commercial fund and other similar operations.

Vulnerabilities

Due to the skills that insolvency practitioners have them in bankruptcy proceedings, they are vulnerable to the risk of being used by money launderers for alienation of part of the assets, to the detriment of the creditors.

There appears to be limited understanding and some reluctance among the sector regarding the enforcement of AML/CTF obligations, considered to be primarily the responsibility of financial institutions, especially banks.

Types of money laundering and typical cases of money laundering related to the sector and high-risk products / services

USE OF ACCOUNTS HELD IN ROMANIA BY RESIDENT NATURAL PERSONS AND LEGAL ENTITIES FOR THE RECYCLING OF AMOUNTS PROCEEDED FROM FORECLOSURE WITH THE SUPPORT OF Bailiffs	
Description	The typology is characterized by the presence of a group of resident natural persons, connected (involved in usury actions), who act on personal accounts opened at resident credit institutions and who carry out several cash withdrawal operations. The resident legal entities involved carried out, as bailiffs, debt recovery activities for resident natural persons. Resident natural persons granted loans using real estate mortgage loan contracts, which were executed, provided that the claims had been fully or partially recovered.
Profile of natural persons/legal entities	Natural persons of average or modest condition, with their residence or domicile in the same area, in absence of fiscal information regarding the income received, these being known by the state bodies as practicing usury. The resident legal entities that recovered the debts were in contact with the natural persons, who practiced usury.
Indicators (type-specific)	- high-value internal transfers made between the accounts of legal entities and resident individuals; - natural persons known to be involved in acts of usury; - multiple operations of cash withdrawals from the account of natural persons below the reporting threshold provided by law;
MECHANISM	• using the accounts of individuals for cash withdrawals; • the involvement of legal entities that have the capacity of bailiff;
INSTRUMENT	• use of cash; • use of bank accounts;

Conclusions

Given that, although there are factors that mitigate the sector's exposure to money laundering risk, such as:

- the fact that these sectors are well regulated from the point of view of the legal framework in force;
- the supervision and control of the way of applying the legislation in the field of AML/CTF is ensured by NOPCML as well as by UNPIR (for insolvency practitioners) and by UNEJ (for bailiffs), as self-regulatory bodies that represent and coordinate them ;
- the existence of fit&proper mechanisms that ensure the maintenance of certain standards regarding access and retention in the profession and that prevent the access to the profession of convicted persons;
- organization by NOPCML of training seminars for professionals in the sector;
- the specificity of the activity carried out by the bailiffs, the inherent risk of the activities carried out being relatively low due to the nature of the services provided;

However, considering aspects such as:

- the level of risk awareness of these professionals seems quite unsatisfactory considering the low number of STRs and the sectors were not controlled;
- the experience of insolvency practitioners as well as the nature of the services provided by them could be useful to money launderers in order to carry out more sophisticated/complex transactions and conclude contracts that legitimize the running of operations that could aim to recycle some funds.

the level of money laundering threat related to these legal professionals is considered to be medium for insolvency practitioners and low for bailiffs.

Bailiffs

No.	Elements	Likelihood Rating (L)	Assessment of consequences (C)	Risk rating
	The risk in the field of bailiffs	**Low**	**Moderate**	**Low**
Associated vulnerabilities: **Some minor deficiencies in the application of anti-money laundering and anti-terrorist financing legislation.** **Bailiffs may face atypical, unusual circumstances regarding activities such as buying and selling undervalued or overvalued real estate.**				
Associated threat: **Running complex operations that can facilitate the concealment of large amounts of money/assets of illicit origin.**				
Event description: **The possibility of keeping fictitious records and buying/selling over/under-valued goods.**				
Risk description: ***It is a low risk*** ***Low probability*** ***Moderate consequences***				

Insolvency practitioners

No.	Elements	Likelihood Rating (L)	Assessment of consequences (C)	Risk rating
	The risk related to insolvency practitioners	**Average**	**Moderate**	**Average**

Associated vulnerabilities: **A relatively low level of awareness regarding how to fulfill the obligation to detect suspicious transactions;** **Certain weaknesses in the enforcement of anti-money laundering and anti-terrorist financing regulations.**
Associated threat: **During the procedure of bankruptcy, it might be possible that insolvency practitioners are used to facilitate fraudulent activities of creditors.**
Event description: **By his powers, the insolvency practitioner could dispose of part of the assets in the bankruptcy proceedings, to the detriment of the creditors.**

Risk description: ***Medium risk*** ***Average probability*** ***Moderate consequences***

4.7.10 Service providers for companies or trusts, other than those provided for in letters (e) and (f)

General description

According to the provisions of art. 5 para. (1) lit. g of Law no. 129/2019 with subsequent amendments and additions, reporting entities are also considered service providers for companies or trusts - other than auditors, accounting experts and chartered accountants, tax consultants, authorized appraisers, persons who grant financial, business or accounting consultancy, etc., notaries public, lawyers, bailiffs and other persons exercising liberal legal professions.

Service providers for trusts, companies and other legal entities or constructions can offer a wide range of services for third parties[122], such as:

1. establish companies or other legal entities;
2. exercise the position of director or administrator of a company or have the capacity of associate of a partnership or a joint venture or a similar capacity within other legal entities or mediate for another person to exercise these functions or capacities;
3. provide a registered office, workplace, commercial, postal or administrative address or any other similar service;
4. exercise the capacity of fiduciary in a trust or similar construction or mediate for another person to exercise this capacity;
5. be a shareholder or arrange for another person to be a shareholder for a legal entity, other than a company whose shares are traded on a regulated market that is subject to advertising requirements in accordance with European Union legislation or set standards internationally.

Current legislation[123] requires reporting entities in the category of service providers for companies and trusts to identify the beneficial owner of clients when entering into a business relationship and to take appropriate and risk-based measures to verify the identity of said beneficial owner. Also, reporting entities in the category of service providers for companies and trusts are required to declare their own beneficial owner in order to be registered in:

- The central register of the ONRC in case they are organized as legal entities that have the obligation to be registered in the Trade Register;
- the Central Register of the National Fiscal Administration Agency in the case of trusts or similar legal constructions.

Service providers for companies or trusts, other than those provided for in art. 5 para. (1) lit. e) and f) of the Law, are entities controlled and supervised by NOPCML.

The main challenges that service providers for companies may face in terms of their obligations in the field of preventing and combating money laundering and terrorist

[122] See the full content of art. 2 lit. l) from Law no. 129/2019 with subsequent amendments and additions
[123] Law no. 129/2019

financing are: lack of policies, rules and procedures adapted to the specifics of each entity's activity, poor application of security KYC measures through risk-based circumstantiation, as well as some non-compliance with the proper fulfillment of the obligation to assess the risks for the clients of each entity.

The processed questionnaires indicate that the entities that were part of the analyzed sample demonstrate that most of them have elusive general knowledge regarding the field of preventing and combating money laundering and terrorist financing and do not know in depth the legislation that applies in the field.

Also, considering the fact that during the analyzed period no suspicious transaction reports sent to NOPCML were identified, we consider that the way of fulfilling the obligation to report suspicious transactions is deficient and it suggests that service providers for trusts and companies might fail to correctly identify high-risk customers or transactions, or fail to properly identify suspected money laundering when it would be reasonable to do so.

General risks of the sector

Money laundering methods and techniques often involve the establishment of legal companies/constructions with complex, opaque structures, structures in which the true identity of the real beneficiaries can be hidden by using intermediaries, which may have the consequence of hindering investigations, difficulties in identifying the person/s who owns or controls the finally the entity and/or the natural person(s) on whose behalf or in whose interest a transaction, operation or activity is carried out, directly or indirectly.

The risk that the services provided by the reporting entities in this sector are exploited by criminals increases when service providers for companies or trusts do not perform the necessary diligence to properly fulfill all obligations arising from the provisions of the legislation regarding the prevention and combating of money laundering/financing terrorism or when a superficial (formal) approach to compliance is adopted, without emphasizing the substance, the actual, spot-on application of the measures that are required in each individual case.

General risks of the products/services offered in the sector

Entities in the corporate or trust service provider sector may be exploited, either knowingly or unknowingly, to facilitate operations that allow significant illicit funds to be laundered through the companies. They often provide services that can facilitate the creation of legal constructs/companies with complex, opaque structures that are attractive to individuals intending to initiate transactions using the proceeds of crime to make it impossible or extremely difficult to link the funds to their illicit origin.

Some of the services provided by this category of reporting entities are exposed to the risk of being used by criminals who intend to launder money, such as: services that involve the exercise of the function of director/administrator of a company or the mediation of the exercise of these functions by a another person, the hosting services of the registered office (the risk increases when a lot of companies are hosted at the same address), the related services consisting in taking over the company's correspondence and sending it to another address. This type of service is also exposed to the risk of attracting non-residents who establish a company on the territory of Romania intending to launder the money obtained

from crimes committed abroad (the method of keeping funds away from the geographical area where the predicate crime was committed), in the context where must have a registered office in Romania to serve as an official address, but the company is not obliged to operate exclusively in Romania.

Other types of services may increase the vulnerabilities of entities in this sector. For example, company service providers can sell so-called "shelf companies" (companies that have been set up by a person who owns them and keeps them running - although usually no business is carried out through them - until finding a buyer, after which ownership is transferred from the supplier to the buyer, who can then start operating through the company he purchased). These products are attractive to criminals because, once purchased, they can more easily disguise money laundering activities by using such structures or by using intermediaries to hide the real beneficiary.

In many cases, the provision of services to companies is not the main activity of the firm, it is often another activity. The interconnection of the provision of services for companies and trusts (services listed in art. 2 letter l of Law no. 129/2019) with other services involves risks in the sense that criminals could request a package of complex services from professionals, in order to identify the way best way to conceal the illicit origin of some assets.

The possible non-compliance with the legislation in the field of preventing and combating money laundering by service providers for companies or trusts can significantly increase the risk regarding the exposure of the sector to the mentioned phenomena, because the failure of the reporting entities to carry out all due diligence in order to fulfill the obligations arising from the provisions of these acts normative can be speculated by people who have funds of illicit origin and who need the experience of professionals in this field to disguise the origin of these assets.

Overall vulnerability of specific sector/products to money laundering risk

The key aspect of the sector's exposure to risk is that intermediaries can be misused by criminal groups to create entities that can be used in money laundering transactions. In other situations, some intermediaries or third parties may offer services that facilitate the concealment of the real beneficiary, such aspects may have a major impact in increasing the risk level of the entire sector regarding exposure to money laundering/terrorist financing phenomena.

General Vulnerabilities:

- interposing in various transactions an entity that is not recently established, seems to have a history in the market and therefore a lower risk than that of a new one, as well as adding a new link in the stratification stage of money laundering;
- services relating to entities in a jurisdiction with less strict regulations, which may facilitate anonymity or opacity, for example matters related to the registration of entities, their supervision, updating information regarding the entity's associates;
- situations where the clients are entities whose structure makes it difficult to identify the real beneficiary in a timely manner, clients who intend to interpose a family member/close person to create distance between the apparent and the real beneficiary, or clients who try to conceal /hide information regarding understanding of the ownership and control structure, their business or the nature of their transactions;

- the situations in which the services requested from the service provider for companies or trusts present connections with certain transactions, structures, geographical areas, activities carried out in several states, or other factors that are not consistent with the information regarding the client's activity or the economic purpose behind the establishment or administration of the client to whom the supplier provides services;
- situations where a client's representative offers the supplier payment of extraordinary fees for certain services, for which such an amount would not normally be paid;
- the sudden intensification of the activity of a client who was previously mostly inactive, without a clear explanation; in general, criminals involved in organized crime activities try to place the illicit capital in a new business market, especially if this market is predominantly cash-based.

Other specific vulnerabilities: the extremely low number of STRs transmitted by entities in this sector; low interest, in some cases, towards the theoretical and practical aspects regarding the prevention of ML/TF; in the case of some of the reporting entities, the staff is insufficiently trained on the relevant aspects of the legislation in the reference area, which leads to the inconsistency of implementing the rules/procedures/policies to prevent and combat money laundering and terrorist financing in this domain; insufficient supervision of the sector.

Fit&proper mechanisms, registration/authorization and surveillance mechanisms

The legislation[124] regarding such companies stipulates that they cannot be established by persons who, according to the law, are incapable or who have been forbidden by a final court decision the right to exercise the capacity of founder as a complementary punishment of conviction for crimes against the patrimony through breach of trust, crimes of corruption, embezzlement, crimes of forged documents, tax evasion, crimes provided for by Law no. 129/2019 or for the crimes provided for by the commercial companies law, Law no. 31/1990 republished.

Persons holding the capacity of fiduciary, as well as persons holding an equivalent position in a legal construction similar to the trust, are obliged to register, within one month from the date of conclusion, the contracts of trust and of legal constructions similar to trusts, as well as the changes them, at the fiscal body in whose fiscal records the appointed fiduciary is registered as a payer of taxes, fees and contributions. In the "Central Register of trusts and legal constructions similar to trusts", NAFA keeps records of trust contracts and legal constructions similar to trusts.

In April 2022, in order to ensure effective supervision and monitoring of the various categories of reporting entities, a new normative act was adopted in Romania (GEO no. 53/21.04.2022[125]) which establishes the obligation including for service providers for companies or trusts provided for in art. 5 (1) letter g) to immediately notify NOPCML regarding the start/cease/suspension of the activity that falls under the provisions established by Law no. 129/2019.

[124]Article 6 paragraph (2) of Law no. 31/1990 on companies.
[125]GEO no. 53/21.04.2022 regarding the amendment and completion of Law no. 129/2019

Types of money laundering and typical cases of money laundering related to the sector and high-risk products / services

USE OF ACCOUNTS HELD IN ROMANIA BY ONE PERSON RESIDENT LEGAL COMPANY, PROVIDING SERVICES UNDER A CONTRACT OF TRUST FOR THE RECYCLING OF PRODUCTS FROM ORGANIZED CRIME	
Description	The typology is characterized by the presence of a resident legal entity that provides services under a trust contract. Through the accounts opened by it, significant sums of money are collected from an association registered in an off-shore jurisdiction, controlled by a resident natural person involved in an organized crime group. The sums collected according to the trust contract were invested in a foreign market (transfers made to a non-resident legal entity), based on the aforementioned contract. Later, the funds were transferred to the resident natural person's accounts with the title investment profit consideration. The typology is characterized by the presence of a resident legal entity that provides services based on a trust contract. Through the accounts opened by it, significant sums of money are collected from an association registered in an offshore jurisdiction, controlled by a resident natural person involved in an organized crime group. The amounts collected under the trust agreement were invested in a foreign market. Thus, transfers were made to a non-resident legal entity, based on the above contract mentioned. Later, the funds were transferred to the resident natural person's accounts with the title investment profit consideration.
Profile of natural person/legal entity	Profile of natural persons/legal entities involved in transactions: resident natural person known to be part of an organized crime group, controlling an association-type legal person established in an off-shore jurisdiction; resident legal entity providing fiduciary services (law firm) with a varied clientele; non-resident legal entity that makes investments on the real estate market where it was registered.
Indicators (type-specific)	- external transfers of significant amounts from an association from accounts opened in an off-shore jurisdiction; - agreement between the credits and debits of the accounts of the resident legal entity; - information regarding the involvement of the resident natural person in an organized criminal group.
MECHANISM	• using the accounts of legal entities that provide services based on a fiduciary contract; • the involvement of an association that operates in an off-shore area;
INSTRUMENT	• using a fiduciary services contract; • use of bank accounts; • the use of external transfers.

Conclusions:

The services offered in this sector by service providers for companies and trusts can often be used by people who intend to launder money. So they:

- can offer services regarding the sale/mediation of transactions of so-called "shelf companies", in order to interpose in various transactions an entity that is not recently established (and for this reason seems to have a history in the market and therefore a lower risk than that of a new one) with the aim of adding a new link in the stratification stage of money laundering.
- may offer services relating to entities in a jurisdiction with less strict regulations, which may facilitate anonymity or opacity, such services being often used by persons intending to launder money;

No.	Elements	Likelihood Rating (L)	Assessment of consequences (C)	Risk rating
	Risk related to service providers for companies and trusts	**Average**	**Major**	**High**
Associated vulnerabilities:				
The services offered in this sector by service providers for companies and trusts can often be used by people who intend to launder money.				
Associated threat: **The establishment of companies/legal structures with complex, opaque structures, structures in which the true identity of the real beneficiaries can be hidden by the use of intermediaries;** **The services can be used by criminals involved in organized crime activities, who are trying to place capital in a new business market, to distance the money as much as possible from its illicit source.**				
Event description: **Entities whose structure makes it difficult to identify the real beneficiary in a timely manner** **Clients interposing a family member/next of kin to create distance between the ostensible and actual beneficiary.** **Entities attempting to disguise/conceal information regarding the understanding of their ownership and control structure, their business or the nature of their transactions.**				
Risk description: ***High risk*** ***Average probability*** ***Major consequences***				

4.7.11 Virtual and Fiat Currency Exchange Service Providers and Digital Wallet Providers

General description

Virtual currencies or cryptoassets are cryptographically secured digital representations of value or contractual rights that use some form of distributed ledger technology and can be transferred, stored or traded electronically. Digital wallet providers are entities that provide safekeeping services of private cryptographic keys on behalf of their customers for the holding, storage and transfer of cryptoassets.

Providers of exchange services between virtual currencies and fiduciary currencies and providers of digital wallets are reporting entities according to the provisions of Law no. 129/2019.

In Romania, starting with 2019, new regulations were introduced in the Fiscal Code regarding the taxation of income from cryptocurrency trading. Thus, natural persons who obtain this type of income have the obligation to declare and pay income tax and social health insurance contributions. Income tax is levied on the gain obtained by the natural

person, i.e. the positive difference between the selling price and the purchase cost, including the costs that can be attributed to the trading of virtual currencies.

According to the provisions of Directive (EU) 2015/849, as amended by the Directive (EU) 2018/843, as of July 15th, 2020, the legislation was amended[126] with the definition of the virtual currency and of the digital wallet provider, the introduction of exchange service providers between virtual currencies and fiduciary currencies and digital wallet providers as reporting entities, as well as the regulation by general provisions of the authorization and/or registration method of providers of exchange services between virtual currencies and fiduciary currencies and providers of digital wallets.

The authorization and/or registration procedure, as well as the procedure for granting and withdrawing the technical approval is established by a Government Decision, developed by the Ministry of Finance together with the Authority for the Digitization of Romania and NOPCML, with the approval of the Ministry of Internal Affairs and the National Authority for Consumer Protection.

The quality of exchange service provider between virtual currencies and fiduciary currencies or digital wallet service provider can be acquired by a Romanian legal entity established according to the legislation or legal entity legally established and authorized/registered by the competent authorities in a member state of the European Union or in the signatory states of the Agreement on the European Economic Area or in the Swiss Confederation.

In April 2022, Romania adopted a new legislative provision (GEO no. 53/21.04.2022[127]) which establishes the obligation of providers of exchange services between virtual currencies and fiduciary currencies and providers of digital wallets to immediately notify NOPCML of the start/stop of the activity that falls under the provisions established by Law no. 129/2019.

Legislation in force[128] requires virtual and fiat currency exchange service providers and digital wallet providers to identify the beneficial owner when entering into a business relationship and to take appropriate risk-based measures to verify the identity of beneficial owners. Also, they are obliged to declare their own real beneficiary in the central register organized at ONRC level if they are Romanian legal entities.

Application of the provisions of the law[129] by exchange service providers between virtual currencies and fiat currencies and by digital wallet providers is supervised and controlled by NOPCML.

The analysis of the cases revealed the presence of 52 instances in which cryptocurrencies were used to recycle the sums of money resulting from the commission of crimes. The main predicate crimes were corruption, IT crimes, fraud, phishing and skimming fraud and tax evasion. External collections represent the main method of introducing money from predicate crimes into the banking system, and the main methods of externalizing recycled money were external transfers and cash withdrawals.

[126] GEO no. 111/2020 amended Law no. 129/2019

[127] GEO no. 53/21.04.2022 regarding the amendment and completion of Law no. 129/2019

[128] Law no. 129/2019

[129] Law no. 129/2019

Providers of exchange services between virtual currencies and fiat currencies submitted to NOPCML, during the period under analysis in this Report, a number of 17 STRs.

Conclusions – Providers of exchange services between virtual currencies and fiat currencies and that of digital wallet providers submitted a small number of STRs, which do not demonstrate a good knowledge of the legislation in this area, but the sector is subject to STRs submitted by financial institutions, these reports being complete and complex.

Although their value may seem volatile and their operation complex, several features make them attractive for money laundering. These features allow money launderers to transfer, integrate and layer illicit funds into cryptoassets, before converting them back into fiat currency, to hide the source and original purpose of the funds and transfer value around the world.

The increasingly obvious orientation of organized crime groups towards money laundering through mining activities and cryptocurrency transactions is favored by the reduced possibilities of institutional control of the environment, anonymization and the lack of traceability of amounts converted into virtual currency (origin and destination), the speed of operations and the absence of limits for the volume of transferred funds.

General risks of the sector

As general risks of the sector, the lack of knowledge and understanding is highlighted, which prevents providers of exchange services between virtual and fiat currencies and providers of digital wallets, as well as the competent authorities to carry out an adequate assessment of the impact of the sector in the matter of ML/TF, as well as gaps or ambiguities in the application of existing regulations.

The sector is not yet fully regulated and it is still difficult to find appropriate tools to provide relevant information to raise awareness.

The NBR has noted the continued trend of increasing public interest in virtual currencies (also known as crypto-assets) and draws attention to the fact that, in its opinion, they continue to represent speculative, highly volatile and extremely risky assets that have a high potential to generate financial losses for investors.

Although, according to the opinions of the European Banking Authority, the risk of illicit use of virtual currencies remains high, premises have been created for their management.

At the same time, at the European level, the process of regulating virtual currencies and related service providers has been started, and negotiations are currently taking place between member states based on the proposal for a Regulation developed by the European Commission on the crypto-assets market.

The manifestation of risks specific to the ownership and trading of virtual currencies and the significant volatility of the price of some traded virtual currencies do not currently represent a threat to financial stability in Romania.

General risks of the products/services offered in the sector

Cryptoasset exchanges are the most common way for consumers to initially enter the cryptoasset market by purchasing, trading and investing in cryptoassets.

ATMs for cryptoassets are also at risk of being abused by money launderers, providing another gateway for criminals to enter the crypto-asset market to launder funds. ATMs can provide criminals with the anonymity to disguise the source of illicit cash by exchanging it in and out of crypto-assets.

Cryptoasset ATMs are potentially more vulnerable to abuse than exchanges because they offer criminals the ability to directly convert held funds into criminal cash, unlike an online cryptoasset exchange where cash can be transferred, usually only through a bank or other regulated payment system.

Peer-to-peer (P2P) exchange platforms are also considered to be at risk of abuse by money launderers and are likely to be used by OCGs. P2P platforms can put users in direct contact over the internet or in physical contact with each other, providing the ability to transfer ownership of cryptoassets using cash without the transaction appearing on the blockchain. Meetings can also be arranged via encrypted messaging, making it difficult for law enforcement authorities to track. The wide range of P2P business models, levels of compliance and rapid evolution mean that risks can vary within the subsector.

The overall vulnerability of the sector to the risk of money laundering and to specific products

Given their online accessibility and global reach – cryptoassets allow criminals to quickly transfer funds across national borders without requiring a face-to-face business relationship.

There are also uneven regulatory requirements and regulatory gaps – some jurisdictions do not require firms that facilitate the exchange of cryptoassets to conduct adequate due diligence on their customers and transactions.

Crypto-assets can also act as a payment method between criminals, can be used to purchase illicit tools and services online, and can be exploited for other criminal activities such as fraud. Crypto assets also remain a key tool in cybercrime. Cryptoassets are suitable for use in cybercrime and are regularly used by cybercriminals to hold and transfer funds.

Another vulnerability, revealed through analyses carried out by law enforcement bodies, is represented by the possibility of anonymizing the recipients of transactions by purchasing virtual currency and transferring money through several anonymized accounts.

Fit&proper mechanisms, registration/authorization and surveillance mechanisms

For this sector, the existing legislation contains anti-money laundering and anti-terrorist financing provisions and has established an obligation for providers of exchange services between virtual and fiat currencies and digital wallet providers to notify NOPCML of the start/stop of activity that falls under the provisions established by Law no. 129/2019, but the authorization mechanisms are not yet established.

Thus, starting on July 15th, 2020, the legislation was amended[130] existing in the sense of the definition of the virtual currency and the digital wallet provider, the introduction of exchange service providers between virtual currencies and fiduciary currencies and digital wallet providers as reporting entities, as well as the regulation by general provisions of the way of authorization and/or registration of providers of exchange services between virtual currencies and fiduciary currencies and providers of digital wallets.

The application of provisions of the law[131] by the providers of exchange services between virtual currencies and fiduciary currencies and by the providers of digital wallets is supervised and controlled by the NOPCML which can also check if the people who hold a management position within these entities reporting persons as well as the persons who are the real beneficiaries of these entities are suitable and competent persons who can protect these entities against their misuse for criminal purposes.

According to the discussions within the Focus Groups, it was highlighted that there could be between 5 and 6 cryptocurrency operators in Romania, although the statistics are not confirmed. It has not been ruled out that these cryptocurrency operators deal with different types of VASPs. Although the cryptocurrency operator sector has explained how to apply know-your-customer measures and monitor activity through blockchain, there are challenges related to identifying the beneficial owners and customers of PEPs. Due to limited oversight of the sector, there is no information on the adequacy and effectiveness of the due diligence measures applied by the sector.

Types of money laundering and typical cases of money laundering related to the sector and high-risk products / services

USE OF ACCOUNTS HELD IN ROMANIA BY NATURAL PERSONS RESIDENCES FOR THE RECYCLING OF FUNDS DERIVED FROM COMPUTER FRAUD AND DECEPTION	
Description	The typology is characterized by the presence of a group of resident natural persons involved in computer fraud crimes, who sold to non-resident natural persons via the Internet very cheap goods that did not physically exist. The collected sums of money were converted into electronic currency, and when the virtual currencies were redeemed, the money was transferred to the accounts of resident natural persons in the form of investment recovery, from where they were withdrawn in cash.
Profile of natural persons /legal entities	Profile of natural persons/legal entities involved in the transactions: resident natural persons who have been the subject of several criminal cases, as a result of committing the crimes of deception and computer fraud. In the case of resident natural persons, there were discrepancies between the incomes declared to the fiscal authorities and the funds transferred through the bank accounts. One of the resident natural persons held the capacity of associate and administrator of a resident legal entity whose business was "wholesale of electronic and telecommunications components and equipment". Resident legal entities that carry out their activity in the field of crypto currency.

[130] GEO no. 111/2020 amended Law no. 129/2019

[131] Law no. 129/2019

Indicators (type-specific)	- non-identification of the real beneficiary of the transactions; - conducting banking transactions with resident legal entities operating on the active, speculative, extremely volatile and risky virtual currency trading market; - multiple cash withdrawal operations.
MECHANISM	• using the accounts of resident legal persons to purchase virtual currencies with proceeds of crime; • the involvement of a cryptocurrency company.
INSTRUMENT	• use of cash; • use of bank accounts; • the use of external transfers.

Conclusions:

Risk mitigating factors in the sector:

The supervision and control of the way of applying the legislation in the field of AML/CTF by this category of reporting entities is ensured by NOPCML, which regularly organizes training sessions dedicated to this sector;

Existence of fit&proper mechanisms – persons holding a management position within providers of exchange services between virtual currencies and fiat currencies and providers of digital wallets, as well as the persons who are the beneficial owners of these entities must be suitable and competent persons who can protect these entities against their misuse for criminal purposes.

Entities in this sector are subject to relatively new regulations at national level, a fact that involves a series of challenges in the sphere of supervision and control, the risk being mitigated by the provisions of GEO 53/2022 which established the obligation of entities in the sector to notify NOPCML about at the start/suspension/termination of the activity.

No.	Elements	Likelihood Rating (L)	Assessment of consequences (C)	Risk rating
	Risk related to virtual and fiat currency exchange service providers and wallet providers Digital	**Very big**	**Moderate**	**High**
Associated vulnerabilities: **The fact that they are provided via the Internet.** **Limited transparency of virtual currency transactions and the identities of individuals involved in these transactions.** **The cross-border element - the fact that they can allow interaction with high-risk areas or with high-risk customers that cannot be easily identified.** **Volatile and complex operations make cryptocurrencies attractive for money laundering. Crypto asset exchanges are a gateway to buying and exchanging fiat currencies.** **Sector awareness of ML/TF risks is still limited given the low number of suspicious transaction reports from this sector.**				
Associated threat: **Cryptoassets allow criminals to quickly transfer funds across national borders without requiring a face-to-face business relationship;** **Crypto-assets are suitable for use in cybercrimes and are regularly used by cybercriminals to hold and**				

transfer funds.
Event description: **Purchasing cryptocurrencies with proceeds of crime.** **Crypto-asset ATMs could be abused by money launderers, providing another entry point for criminals to enter the crypto-asset market for the purpose of laundering funds.** **Anonymizing transaction recipients by purchasing virtual currency and transferring money through multiple anonymized accounts.**
Risk description: ***High risk*** ***Very high probability*** ***Moderate consequences***

4.7.12 Real estate agents and developers

General description

The contribution of real estate transactions to GDP formation is 8% (representing 84,721 million lei), according to statistical data received by NOPCML.

Taking into account the declared main field of activity, 10,666 real estate agencies are registered with ONRC - 9,102 legal entities and 1,564 authorized natural persons. The data and information were provided by ONRC only for active entities for the period 31.12.2020 – 20.01.2021 and have a margin of error of 5%.

The legal entities that declared on 31.12.2019, income from CAEN code 4110 (real estate development) are 6,010 real estate developers, according to the data received from the Ministry of Finance.

In Romania, real estate agencies and real estate developers do not have specific regulations. They can be established both as a natural person, as well as an authorized natural person or commercial company based on the company law[132]. Also, activities specific to real estate agents can be carried out by any other liberal professions, for example lawyers / law firms.

Specific legislation[133] regarding the incorporation of companies provides that such companies cannot be established by persons who, according to the law, are incapable or who have been forbidden by a final court decision the right to exercise the capacity of founder as a complementary punishment of conviction for crimes against patrimony through breach of trust, crimes of corruption, embezzlement, crimes of forgery in documents, tax evasion, crimes provided for by Law no. 129/2019 or for the crimes provided by the company law.

The manner of application of the provisions of the law[134] by real estate agents and developers is supervised and controlled by NOPCML.

[132] Law no. 31/1990 on companies
[133] Article 6 paragraph (2) of Law no. 31/1990 on companies
[134] Law no. 129/2019

In April 2022, Romania adopted a new legislative provision (GEO no. 53/21.04.2022[135]) which establishes the obligation of real estate agencies and real estate developers (as defined in Law no. 129/2019) to immediately notify NOPCML of the start/suspension/termination of the activity that falls under the provisions established by Law no. 129/2019.

Real estate agencies facilitate the buying and selling of properties and therefore real estate agency services pose a risk of money laundering. Their relationships with both property buyers and sellers can provide crucial information to identify suspicious transactions. The real estate agent is an employee of a real estate agency who is usually paid on commission and whose activity is the mediation of the sale/purchase of real estate, as well as the mediation of real estate rentals.

In Romania, it is not mandatory for the sale/purchase of properties to be carried out through a real estate agency, but the authentication of the sale/purchase contract by a public notary is mandatory.

Real estate developers carry out the development of construction projects for residential and non-residential buildings by bringing together financial, technical and physical means for the realization of construction projects with a view to subsequent sale (this activity does not include building construction, architecture and management activities and management services for building construction projects). Specifically, the real estate developer is the one who has money and invests it in building a residential complex/office building/commercial space/etc. through a legal entity, which it later sells or rents.

The cadastral register and the land book form a unitary and mandatory system of technical, economic and legal records of national importance, of all real estate throughout the country.

The cadastral register carries out the identification, measurement, description and registration of immovables in cadastral documents and their representation on cadastral maps and plans, and the land book includes the description of immovables and the entries related to real estate ownership, personal rights, acts, facts or legal relationships that have related to real estate.

The analysis of the cases highlighted 66 instances in which the real estate market was used in order to recycle the sums of money derived from the commission of crimes. The main predicate crimes were fraud, tax evasion and corruption. External collections represent the main method of introducing the money from the predicate crimes into the banking system, and the main methods of externalizing the amounts of recycled money were external transfers and cash withdrawals.

The analysis highlighted specific cases regarding the operating mode of the OCGs in Romania on the real estate market, such as: various maneuvers involving the overestimation of the market value of real estate obtained fraudulently and which end up in different forms (e.g.: contribution to the capital) in the patrimony of the companies owned or controlled through intermediaries by the members of the groups in question, their mortgage (with the complicity of authorized appraisers/bank officials) in order to obtain bank loans that can reach millions of euros, the committed credits being returned from the

[135]GEO no. 53/21.04. e

amounts of illicit origin introduced into the economic circuit with the title of financing/associate.

Organized crime groups invest directly, by lending to controlled companies whose activity is the construction of residential complexes, or by purchasing them (directly or through intermediaries) at prices well below market levels (most often through fraudulent maneuvers with the co-interested support of local government officials, bailiffs, notaries public, bank officials). They then resort to successive trading of the properties with an increase in value, in order to justify the obtaining of large sums of money by the persons involved in the fictitious circuit and, eventually, the final valuation on the property market. As regards transactions in disputed rights, organized crime groups initially purchase them at modest values and then successively remarket them at increased value, paying for them with funds of illicit origin. Examples of law enforcement investigations include: money obtained from bribes taken as a public official, which is then reinvested in real estate; fraud in public procurement by overvaluing and then investing the money obtained in real estate; obtaining illicit funds (bribery and abuse of office when overvaluing contracts), repeated transfers of illicit money (bribery, overvaluing contracts) through the accounts of offshore companies, cash withdrawals and investments in commercial/real estate activities of trusted persons.

Examples of law enforcement investigations (in cases of tax evasion and embezzlement) involving real estate include the following:

- defendants who used a significant part of the sums obtained as a result of tax evasion activities, carried out through several legal entities that carried out online trade with consumer products, for the purchase of real estate. In order to conceal the true nature of the ownership of the goods or the rights over them, but also to prevent the risk of the establishment of insurance measures, the buildings were purchased in the name of interposed persons, the necessary financial resources being made available by the defendants;
- real estate investments through third parties and the non-declaration of notarial documents of real estate purchases, followed in time by repeated trading through intermediaries.

The modus operandi (mentioned in the questionnaires) includes: massive cash withdrawals from the accounts of some companies based on forged supporting accounting documents, followed by investments in real estate properties paid in cash, in the names of the administrator's family members; illegal VAT refunds, followed by the subsequent investment of illegally obtained money in real estate.

Other typologies include: the members of the criminal group acted to identify people who wanted their real estate ownership rights restored, or to identify unclaimed real estate or assets that were not the subject of property rights restoration. Later, by forging some documents/ownership deeds and by obtaining false statements from materially interested persons, they obtained final court rulings by which they were recognized/granted the right of ownership over some real estate.

From the case file and the analyses carried out by the law enforcement bodies, various cases were presented in which the money obtained from corruption crimes and other similar crimes (abuse in office, fraud, tax evasion or illicit funds obtained abroad through fraud, pimping, trafficking of people) were laundered through real estate investments.

Also, the law enforcement bodies indicated as sources of illicit funds laundered through the real estate sector:

- The construction industry (from large infrastructure projects to real estate developers – through tax evasion, smuggling), funds being laundered through the banking system with false documents certifying fictitious operations, etc. and integrated through real estate investments;
- Money from the underground economy (smuggling, tax evasion, human trafficking, pimping/prostitution) is placed in the financial banking sector and then integrated into the real estate sector;
- External/internal funds from the facilitation of prostitution are transferred through successive operations (successive transfers through several bank accounts or through money transfer services, regulated or not) and are subsequently invested in the real estate sector;
- Proceeds from the commission of crimes transferred to relatives and close persons and later withdrawn in cash and invested in immovable and movable property;
- Situations in which the real estate was purchased by non-resident companies with funds derived from the commission of crimes in order for the assets to be transferred to the members of the organized criminal group through the conclusion of loan agreements;
- Embezzlement, the proceeds of crime being transferred by the members of the organized criminal group to non-resident companies that purchased real estate (office buildings) and rented them, so that the invested criminal proceeds generated future rental income through the non-resident company for the members of the organized criminal group;
- Sums of money obtained from committing economic crimes are invested abroad (Spain, the UK) in the purchase of real estate (houses, boarding houses, hotels), the real estate being used by organized crime groups, and the sums of money being reinvested in the country.

In general, from the supervision and control activities, it was found that real estate agencies have many shortcomings in the application of anti-money laundering and anti-terrorist financing measures, limiting measures to mitigate the risk of money laundering in this sector. The main common challenges identified are the lack of customized policies, controls and procedures, the application of risk-based circumstantial customer due diligence measures and the appropriate risk assessment for each entity's customers.

Conclusions –Real estate agents and developers, during the period analyzed in this report, do not appear to have sent any STRs to the NOPCML, which disproves a good knowledge of the legislation in this field. Financial institutions submitted STRs that formed the basis of NOPCML's analyses, providing an overview of the sector.

From the processed questionnaires, it emerged that most of the entities that were part of the analyzed sample have elusive general knowledge in the field of combating money laundering and terrorist financing and do not have a thorough knowledge of the applicable legislation in this field.

General risks at sector level

The real estate sector faces a high risk of money laundering, as the purchase of real estate remains an attractive method for laundering illicit funds due to the large sums that can be

transferred or invested in this sector and the low levels of ownership transparency or source of funds.

Also, acquisitions made by legal entities with complex or opaque structures in offshore areas to hide ownership, which makes unclear the true purpose and origin of the financial transactions involved, present the highest level of risk, due to the difficulties in establishing of the final beneficiaries.

Properties can be purchased through several intermediaries. In addition to those subject to AML/CTF supervision, there may be persons responsible for selling property who are not subject to these rules, such as housebuilders, who may sell property directly to the customer. This provides opportunities for purchasing properties without any verification of the buyers or their source of funds. Given the high values involved in a real estate investment, the domain is preferred, which facilitates the laundering of large sums of money. The mode of operation is relatively simple, through real estate transactions, real estate development or obtaining litigious rights.

The nature of transactions in the real estate market, involving various regulated professionals, may influence the estate agency to rely on other persons, such as lawyers or notaries, to apply due diligence measures, considering that the risk or responsibility rests with other persons involved in trial.

General risks of the products/services offered in the sector

Criminals often buy property as a long-term investment and to use the proceeds of crime. The large sums of money that can be transferred in a single transaction and the appreciation of property values, along with the luxury lifestyle, make them very attractive to criminals.

Properties are also bought and sold as a method of layering the proceeds of crime. Criminals can reverse trades, manipulate values, and return to buying and reselling in short periods of time. While the speed of movement of funds involved in property acquisition is slow compared to other methods, the large sums of money that can be involved and the accessibility of the sector make property sale/purchase an attractive method of money laundering.

Selling/buying property can facilitate money laundering due to its high value and ability to disguise large sums of money as legitimate business transactions.

Rental activities are subject to the law[136]only with regard to transactions for which the value of the monthly rent represents the equivalent in lei of EUR 10,000 or more. Land and rental properties that exceed this threshold are considered attractive for money laundering due to their high value. However, money laundering can also be facilitated at lower rent properties. Money launderers could use small amounts of money to disguise their presence in this sector.
Considering this, the understanding of the risks in this sector is still limited.

[136]Law no. 129/2019

The volume of funds that can be laundered through rental properties varies greatly by location and type of property. Thus, significant amounts of money can be transferred regularly (usually monthly).

The overall vulnerability of the sector to the risk of money laundering and to specific products

Real estate agents are usually involved in a business relationship with other professionals (such as notaries, lawyers, etc.), which makes it difficult to effectively monitor the business relationship (sectors rely on each other to do checks) and therefore increases risk exposure. Real estate activities may rely on non-EU financial flows and high-risk clients such as publicly exposed individuals.

Criminal assets are generally held in cash (a situation often encountered in law enforcement investigations), often invested in real estate (construction of residential complexes or hotels, land, housing, vacation homes, offices), in the name of other persons or in private businesses (in the field of services).

Suspicious transaction reporting is patchy and relatively satisfactory only when carried out by obliged entities other than estate agents – for example, banks (estate agents seem to consider that as they are not involved in the transfer of funds they are not responsible for transaction reporting suspicious). Verifications are difficult to perform as this is an unregulated area.

Other specific vulnerabilities: lack of STRs sent to NOPCML; deficiencies regarding staff training at the level of the reporting entities, which leads to an inconsistent application of policies to prevent and combat money laundering and terrorist financing in the field.

The real estate sector can be used by OCGs to launder money obtained through illegal activities in Romania, especially as a result of tax evasion.

Conclusions:

Real estate agencies have connections with other professionals (lawyers, notaries, accountants, etc.). A factor mitigating the risks specific to the real estate sector is the fact that the value of the sums involved in real estate transactions carried out in Romania is not as high as that of transactions carried out in other more developed EU countries, due to the lower level of population income.

The level of awareness of money laundering or terrorist financing risks in the sector varies according to the size of the entity. Thus, larger entities are more aware of the aforementioned risks compared to small operators who are not aware of exposure to money laundering and terrorist financing risks.

As part of the sector's surveillance activities, non-compliance with the legal provisions was identified, with an emphasis on the following aspects: the lack of personalized policies, controls and procedures, the application of risk-based KYC measures and the adequate assessment of risks for the customers of each entities.

Investments in the real estate sector can often be used by criminals or their agents in money laundering schemes.

Considering the large number of entities operating in this sector, a specific legal framework is necessary to prevent the abusive use of the sector by money launderers.

Risk mitigating factors in the sector:

For this sector, the existing legislation contains provisions related to combating money laundering and terrorist financing and establishes the obligation of reporting entities in the sector to notify NOPCML regarding the start/stop of the activity that falls under the provisions established by Law no. 129/2019.

The supervision and control of the way of applying the legislation in the field of AML/CTF by this category of reporting entities is ensured by the NOPCML, which also periodically organizes training sessions dedicated to this sector.

No.	Elements	Likelihood Rating (L)	Assessment of consequences (C)	Risk rating
	Risk related to real estate agents	**Average**	**Major**	**High**
Associated vulnerabilities: **In Romania, real estate agencies do not have specific regulations and are not coordinated by a self-regulatory body.** **The degree of awareness of the sector regarding the risks of ML/TF still seems to be limited considering the lack of reports of suspicious transactions originating from this sector; Law enforcement bodies have identified cases where the money obtained from crimes was laundered through real estate investments.**				
The identification, within the supervision activities of the sector, of non-compliance with the legal provisions				
Associated threat: **Large amounts of money that can be transferred in a single transaction.** **Ability to cancel trades, manipulate values and return to buying and reselling in short time frames.**				
Event description: **Criminals often buy property as a long-term investment and to use the proceeds of crime.** **Real estate purchases made by legal entities with complex or opaque structures from offshore areas present a high level of risk, as such operations can aim to hide the true owner of the goods, making both the real purpose of the investment and the origin of the amounts involved in the financial transactions unclear.**				
Risk description: ***High risk*** ***Average probability*** ***Major consequences***				

4.7.13 Persons trading art or acting as intermediaries in the art trade and persons storing or trading art or acting as intermediaries in art trading, including when this activity is carried out by art galleries and auction houses or in free zones, if the value of the transaction or a series of related transactions represents the equivalent in lei of at least EUR 10,000

General description

General supervisory framework

In accordance with the legal provisions, persons who trade works of art or who act as intermediaries in art trading and persons who store or trade art or who act as intermediaries in art trading, including when this activity is conducted by art galleries and auction houses or in free zones, are considered reporting entities if the value of the transaction or a series of related transactions represents the equivalent in lei of at least EUR 10,000.

This category of activities can be carried out both by natural persons, as well as by authorized natural persons or commercial companies based on the company law[137].

According to the provisions of Law 31/1990 on companies[138], persons who, according to the law, are incapable or who have been convicted for fraudulent management, abuse of trust, forgery, use of forgery, fraud, embezzlement, perjury, giving or taking bribes, for the crimes provided for by the Law, cannot be founders in order to prevent and sanction money laundering, as well as for the establishment of measures to prevent and combat the financing of acts of terrorism, with subsequent amendments and additions, for the offenses regarding the insolvency procedure.

For this category of reporting entities, in Romania there is no self-regulatory body, therefore the application of the provisions of law 129/2019 is supervised and controlled by NOPCML as part of its duties.

According to Romanian legislation[139], works of art are:

1. paintings, collages and similar decorative plaques, paintings and drawings, executed entirely by hand, other than architectural, engineering plans and drawings and other industrial, commercial, topographical or similar plans and drawings, original, hand-made, manuscript texts, photographic reproductions on sensitized paper and carbon copies obtained from the plans, drawings or texts listed above and hand-decorated industrial articles;
2. engravings, prints and woodcuts, old or modern originals, which were shot directly in black and white or color, of one or more plates/plates executed entirely by hand by the artist, regardless of the process or material used, without including mechanical or photomechanical processes;
3. original productions of statuary art or sculpture, in any material, only if executed entirely by the artist; copies executed by an artist other than the author of the original;
4. tapestries executed by hand according to original models provided by the artist, provided that there are no more than 8 copies of each;
5. individual ceramic pieces executed entirely by the artist and signed by him;
6. enamels on copper, executed entirely by hand, in no more than 8 numbered copies bearing the artist's signature or the name/name of the workshop, with the exception of gold or silver jewelry;
7. photographs executed by the artist, printed on paper only by him/her or under his supervision, signed, numbered and limited to 30 copies, including all sizes and mounts.

[137]Law no. 31/1990 on companies

[138]Art. 6 of (2) of Law 31/1990

[139]Article 312 paragraph (1) letter (a) – Law no. 227/2015 regarding the Fiscal Code

Public sale of works of art[140] (movable cultural goods) in private ownership, or the intermediation of the sale, is carried out only through authorized economic operators, in compliance with the provisions of Law no. 182/ 2000 on the protection of movable cultural heritage, with subsequent amendments and additions. Economic operators are authorized by the Ministry of Culture, with the approval of the National Commission of Museums and Collections, in compliance with the rules regarding trade in movable cultural goods.

Economic operators authorized to sell movable cultural assets belonging to the national cultural heritage must keep a register in which the name and address of the bidder, the description and the price of each asset are correctly and completely mentioned. The information contained in the register is confidential.

The economic operators authorized to sell movable cultural assets are obliged to notify in writing, within 5 days from the date of the offer, the decentralized public services of the Ministry of Culture regarding the existence of goods likely to be classified.

Individuals or legal entities under private law, owners of classified movable cultural assets, must notify in writing the decentralized public services of the Ministry of Culture within 15 days from the date of the transfer of such an asset into the ownership of another person, as well as from the date of establishment of a real right over such an asset.

In the event of the loss or theft of classified movable cultural assets, the owners, holders of other real rights, holders of the right of administration, as well as holders with any title of these assets have the obligation to notify, in writing, within 24 hours of finding, the police body in their territorial area.

If during a criminal investigation, carried out in accordance with the law, indications are discovered that a cultural asset, which is located on the territory of the Romanian state, has illegally left the territory of a member state of the European Union, the Prosecutor's Office attached to the High Court of Cassation and Justice notifies to the interested state, under the conditions of the Law no. 302/2004 on international judicial cooperation in criminal matters, republished, with subsequent amendments and additions.

The analysis carried out in the Report showed that no STRs were sent to NOPCML from this sector of activity.

In the analyzed period, the art objects/cultural goods sector is present and appears in two convictions, theft being the predicate crime. During the laundering process, cash was used (cash deposits/cash remittances) and the proceeds of crime were invested in property (property purchases).

Law enforcement authorities investigated a number of cases involving the use of works of art: Thus, goods from the national cultural heritage originating from theft were purchased with cash, being subsequently introduced into the legal circuit through a company in the UK, a part of the goods being sold in the USA. The goods were illegally taken out of the country, sold on the legal antiquities market, using false documents of provenance, through a UK company owned by the perpetrator of the money laundering offence. The money obtained

[140] goods belonging to the national cultural heritage

from the sale of the goods was reinvested by purchasing other such goods and used for their own needs.

The authorities also indicated cases in which illicit funds resulting from the commission of crimes in various sectors were subjected to the laundering process through the banking system, using false documents certifying fictitious operations, the funds being later integrated into the real economy through investments in works of art and in luxury goods.
In April 2022, Romania adopted a new legislative provision (GEO no. 53/21.04.2022[141]) which establishes the obligation of persons trading/storing or acting as intermediaries in the trade in works of art, including when this activity is carried out by art galleries and auction houses or in free zones, if the value of the transaction or a series of transactions related is the equivalent in lei of at least EUR 10,000, to immediately notify NOPCML regarding the start/suspension/cessation of the activity that falls under the provisions established by Law no. 129/2019.

The Romanian art market registered an upward trend in 2021, noting that in addition to the mix of traded works of art and collectibles, the profile of the collector has also evolved, with works of art being paid for even in cryptocurrencies, and the online has become the new way to buy art. The top 10 auction transactions of 2021 totalled €1.23 million, compared to a total of €1.16 million in 2020, a 6% increase in the average value of a major transaction compared to 2020[142].

Conclusions

From the processed questionnaires, in accordance with the NRA methodology, it emerged that the entities that were part of the analyzed sample demonstrate that most of them have unstructured general knowledge in the field of combating money laundering and terrorist financing and do not have an in-depth knowledge of the applicable legislation in this field.

General risks of the sector

The following risk scenarios can be identified for the trade in art objects:

Criminals can earn income by selling stolen art, artefacts and antiquities. Trafficking in cultural goods is among the largest categories of criminal trade, estimated to be the third or fourth largest. However, there are no instruments to measure legal trade or data on the extent of illicit trade (the specific characteristic of this illicit trade being that it merges with the legal one). Thus, it can be said that there are almost no data or tools for quantifying illicit trade. According to the analysis carried out by the authorities, the black market in works of art is becoming as profitable as that of drugs, weapons and counterfeit goods.

The value of illegal antiquities trafficking is also difficult to assess due to its hidden and continuous nature. It is estimated that only 30-40% of antiques transactions take place through auction houses, where pieces are published in catalogues. The difference is traded through private transactions (often unmonitored and unrecorded).

[141] GEO no. 53/21.04.2022 regarding the amendment and completion of Law no. 129/2019
[142] The 2021_romanesti_art_market_report.pdf

Art is comparable to a commodity and as such can be used in trade-based money laundering to transfer valuable goods across borders. In this way, the proceeds of crime can be relocated or transferred without using a bank to simply transfer funds that criminals know are being monitored for suspicious activity.

The COVID-19 pandemic has brought a new element to the art trade, with the answer being to move operations online. The increasing use of digitized sales platforms has opened up art sales to a greater number of potential buyers from around the world. Thus, the effect of the COVID-19 pandemic has led to an increased risk of abuse of the art market, with an increased use of online platforms, with criminals seizing the opportunity to exploit this type of business.

Regarding the art trade, the following threats can be identified:

The links between the art/antiquities trade and drug, wildlife and arms trafficking, money laundering and tax evasion have been widely reported, placing the antiquities trade at the level of serious transnational organized crime.

Conclusions:

The assessment of the money laundering threat posed by the trafficking of stolen art/artifacts and antiquities shows that this risk scenario can be of interest to organized crime groups, as these "products" can be converted into cash to launder the proceeds from crimes or to avoid paying taxes. Law enforcement officers believe that this type of traffic occurs mostly in free zones and that this makes it difficult to measure the extent of the phenomenon.

In addition, free zones offer a number of customs and tax advantages, which make them more susceptible to crime or abuse. Goods from free zones are subject to EU customs duties and indirect taxes only if they are actually physically brought into the EU territory.

In terms of direct taxation, the lack of transparency about what goods are held in free ports and who owns the goods, can increase the likelihood of tax evasion.

Conclusion: This risk scenario can be an attractive tool for OCGs to convert proceeds of crime into clean cash. However, it requires a high level of experience and is not a safe activity for them. Therefore, the money laundering threat level related to the trafficking of art objects, artifacts and antiquities is considered medium.

Regarding the art trade, the following vulnerabilities can be identified:

The money laundering vulnerability assessment of the trafficking of stolen art, artefacts and antiquities shows that this risk is currently only emerging, but may increase in the short term.

In the sector, cash transactions (sometimes large amounts) are preferred, but online transactions are also widespread, without the financial institution being able to identify the true owner/buyer of the artefacts. There is no specific transaction monitoring.

Customs authorities have difficulties in detecting the illicit origin of cultural artefacts.

Types of money laundering and typical cases of money laundering related to the sector and high-risk products / services

USE OF ACCOUNTS HELD IN ROMANIA BY A RESIDENT INDIVIDUAL FOR THE RECYCLING, THROUGH THE PURCHASE OF ART, OF THE PROCEEDS OF THE OFFENCE OF CAPITAL MARKET MANIPULATION	
Description	The typology is characterized by the presence of a resident individual who collects large sums of money from a non-resident individual under the title of "loan repayment" (the date of the loan being 18 years before the loan repayment). The resident individual transfers the funds received to a non-resident legal person in an offshore jurisdiction under the justification "purchase of art". Data obtained from the jurisdiction where the non-resident individual resides showed that the non-resident individual has been involved, through a non-resident owned legal person, in capital market manipulation and is also listed in the art asset register with a work of art traded by the resident individual, demonstrating that the proceeds of crime have been recycled through the purchase, through intermediaries, of works of art.
Profile of natural person /legal entity	Resident natural person with modest declared income that does not justify the economic behavior, non-resident natural person with substantial declared income and involved in capital market manipulation crimes. The non-resident legal person who is an operator on the market of art objects. The non-resident natural and legal persons involved used accounts opened in a jurisdiction with an uncooperative banking system.
Indicators (type-specific)	- foreign collection of high value in an off-shore jurisdiction; - cashing out with high value after a long period of account inactivity;
	- inconsistency between the explanations provided by the resident natural person regarding the amounts collected and the information resulting from the supporting documents presented; - the inconsistency between the profile of the resident natural person and the banking operations performed.
MECHANISM	• use of an individual's accounts to recycle proceeds of crime through the sale of works of art; • use of a loan agreement entered into 18 years before repayment.
INSTRUMENT	• use of bank accounts; • the use of external transfers

<u>Conclusions</u>:

The Money Laundering Vulnerability Assessment of Traffic in Stolen Works of Art, Artifacts and Antiquities shows that the market for works of art, artefacts and antiquities tends to favor informal channels where there is no security or specific monitoring of transactions. It involves cash payments (sometimes large amounts) where identification of the buyer is almost impossible. The sector appears to be unaware of the risk of money laundering, given the lack of suspicious transaction reports submitted by entities in the sector.

As a result of the new legislative provisions (GEO 53/2022), the entities in the sector will be able to be better identified and supervised by NOPCML, due to the establishment, for this type of entities, of the obligation to immediately notify NOPCML regarding the start/suspension /termination of the activity that falls under the provisions established by Law no. 129/2019, however, considering the following aspects:

- The art trade is an attractive sector for money laundering, requiring a high level of expertise and more elaborate training than other sectors;
- The trading of works of art, artefacts and antiquities is largely done through private transactions;
- For this category of reporting entities there is no self-regulatory body;
- Following the analysis of the sample of entities in the sector, it was found that most of them have unstructured general knowledge in the field of combating money laundering and terrorist financing and do not know in depth the applicable legislation in this field, we consider that the sector presents a medium risk;
- In the period 2018-2020, there are two convictions for dealing in art/cultural goods, and cash and real estate were used to hide the proceeds of crime.

therefore, the level of vulnerability to money laundering generated by the purchase of works of art, artefacts and antiquities is considered average.

Risk mitigating factors in the sector:

For this sector, the existing legislation contains provisions related to combating money laundering and terrorist financing and established the obligation of the reporting entities in the sector to notify NOPCML regarding the start/stop of the activity that falls under the provisions established by Law no. 129/2019.

The supervision and control of the way of applying the legislation in the field of AML/CTF by this category of reporting entities is ensured by the NOPCML, which periodically also organizes training sessions dedicated to this sector.

No.	Elements People who sell works of art	Likelihood Rating (L)	Assessment of consequences (C)	Risk rating
	The risk related to art dealers	**Average**	**Moderate**	**Average**
Associated vulnerabilities: **Non-existence of a self-regulatory body;** **The degree of awareness of the sector regarding the risks of ML/TF still seems to be limited considering the lack of reports of suspicious transactions originating from this sector; Law enforcement authorities have investigated a number of cases involving the use of works of art;** **The black market of the art trade is very attractive to people with illicit funds and money launderers;** **Cash payments are used in the sector (sometimes with large amounts), in these conditions identifying the buyer is almost impossible;** **The increasingly frequent use of digitized sales platforms has provided opportunities for a growing number of potential buyers of art objects around the world.**				
Associated threat: **Customs authorities have difficulties in detecting the illicit origin of cultural artefacts.**				
Event description: **The national cultural heritage goods resulting from the theft were purchased with cash and then introduced into the legal circuit through a non-resident legal entity; the goods were illegally taken out of the country after which they were sold using false documents of provenance; laundering the money obtained from these activities**				

criminal activity was completed by reinvestment, respectively by the purchase of other such goods or goods/services intended for the personal use of the perpetrators;
Risk description: ***Medium risk*** ***Average probability*** ***Moderate consequences***

4.7.14. Other persons who, as professionals, trade goods, only to the extent that they carry out cash transactions whose minimum limit is the equivalent in lei of EUR 10,000, regardless of whether the transaction is executed through a single operation or through several operations that have a connection between them

General description

Apart from the regulated reporting entities, the law does not allow cash operations over 10,000 lei by legal entities, authorized natural persons, sole proprietorships, family businesses, freelancers, natural persons carrying out activities independently, associations and other entities with or without legal personality.

At the same time, the legislator established a maximum threshold for collection and payment operations between natural persons, carried out as a result of the transfer of ownership of goods or rights, the provision of services, as well as those representing the granting/repayment of loans, can be carried out within the limit of a daily ceiling of 50,000 lei/transaction[143].

In the NOPCML case analysis module, the sector "other persons who, as professionals, trade goods, only to the extent that they carry out cash transactions whose minimum limit is the equivalent in lei of 10,000 euros, regardless of whether the transaction is executed through a single operation or through several operations that have a connection between them" was not identified as a distinct sector.

General risks at sector level

Although the provisions of Law No 70 of 2 April 2015 as subsequently amended and supplemented provide for a series of measures to strengthen financial discipline on cash receipts and payments made by legal persons, authorized individuals, sole proprietorships, family businesses, self-employed persons, self-employed individuals, associations and other entities with or without legal personality, with a migration towards less cash-intensive use, the incidence of cash transactions remains high. Thus, there are still risks that criminals may try to use cash-intensive businesses in an attempt to disguise the illicit origin of some funds, for example by commingling them with those of lawful origin.

In April 2022, Romania adopted GEO no. 53/21.04.2022[144] which establishes the obligation of "other persons who, as professionals, trade goods, only to the extent that they carry out cash transactions whose minimum limit is the equivalent in lei of 10,000 euros, regardless of whether the transaction is executed through a single operation or through more many operations that have a connection between them", to immediately notify

[143]Art. 10 of Law no. 70 of April 2, 2015, with subsequent amendments and additions
[144]GEO no. 53/21.04.2022 regarding the amendment and completion of Law no. 129/2019

NOPCML about the start/suspension/termination of the activity that falls under the provisions of Law no. 129/2019.

Risk mitigating factors in the sector:

The provisions of Law no. 70 of April 2nd, 2015 to strengthen financial discipline regarding cash receipts and payments, according to which cash receipts/payments can be made subject to the ceilings established by this regulatory framework.

For this sector, the existing legislation contains provisions related to control money laundering and terrorist financing and established the obligation of reporting entities in the sector to notify NOPCML regarding the start/suspension/cessation of the activity that falls under the provisions established by Law no. 129/2019.

The supervision and control of the way of applying the legislation in the field of AML/CFT by this category of reporting entities is ensured by the NOPCML, which periodically also organizes training sessions dedicated to this sector.

No.	Elements	Likelihood Rating (L)	Assessment of consequences (C)	Risk rating
	Risk relating to other persons who, as professionals, trade goods	**Average**	**Moderate**	**Average**
Associated vulnerabilities: **In Romania, the entities within the sector are not coordinated by a self-regulatory body.** **The degree of awareness of the sector regarding the risks of ML/TF still seems to be limited considering the lack of reports of suspicious transactions originating from this sector; Criminals can sometimes try to place significant amounts of cash by purchasing goods, or integrate laundered money by making investments, calling on professionals who trade in various commodities.**				
Associated threat: **Criminals may try to use cash-intensive businesses in an attempt to disguise the illicit origin of funds, for example by mixing them with those of licit origin.**				
Event description:				
In the integration stage of money laundering resulting from crimes such as tax evasion, fraud, corruption, etc., concrete investments are often made through the purchase of luxury goods (such as jewelry made of precious metals and precious stones, works of art, etc.)				
Risk description: ***Medium risk*** ***Average probability*** ***Moderate consequences***				

V. CROSS-BORDER RISK

5.1 Considering that Romania is not a financial center, the exposure to the risk of money laundering is limited as a result of the fact that large sums of money or those originating from abroad can be easily observed in the system. But there are indications that some criminal groups from neighboring countries are investing in Romania, primarily due to its geographical position, Romania is in danger of being a transit zone for the trafficking of drugs, weapons, stolen vehicles and people.

The main threat in terms of money laundering is posed by criminal groups of Romanian origin operating abroad (cybercrime, trafficking in human beings and drugs, theft) and those operating domestically (tax evasion, corruption). As regards the exposure of the Romanian

financial system to the risk of money laundering, the vulnerability lies in the use of Romanian financial institutions by foreign criminal groups for the transit of illicit funds. These operations are specific both to the stage of placement of sums in the financial system by domestic criminals and to the layering stage (transfer of money between accounts to hide its origin and to make investigations more difficult by involving different jurisdictions). Cross-border crimes are on an increasing trend. The most common transaction pattern is where the predicate offence was committed abroad (mainly in EU Member States) and the money was transferred to accounts opened in Romania and then redirected, mainly to accounts opened with banks in offshore jurisdictions or banks in the Asian region. Another typology that has been observed in cross-border crime is that where wire transfers have been subject to cash withdrawals in Romania. This typology was found in 13 cases. The sectors used for money laundering in the above mentioned cases were trade, cryptocurrencies, medical services and construction.

In terms of international cooperation, the NOPCML receives requests for information from other jurisdictions and sends requests for information to other states in order to gather the information needed to complete the analyses. Thus, in 2018, the NOPCML received 340 requests for information from other jurisdictions, with the most frequent requests being received from Germany (33), the United Kingdom and Austria (28) and Italy (27). In 2019, the total number of applications received from other jurisdictions amounted to 443, with the most frequent applications received from Italy (41), Australia (37), Malta (36) and Germany (24), 390 applications of information submitted by other jurisdictions were received in 2020, with the most frequent requests coming from Germany and Malta (57), Italy (27), Australia (24) and Luxembourg (23).

In 2018, NOPCML submitted 349 requests for information, the main beneficiary countries of these requests were: Italy (41), Cyprus and the USA (21), Switzerland (19) and the United Kingdom (18). In 2019, the main states to which NOPCML sent requests for information were: Italy (40), Cyprus (52), United Kingdom (45) and Bulgaria (37). The total number of information requests sent by NOPCML in 2019 was 731. In 2020, Romania sent a total of 596 information requests. The main beneficiary states of the request sent by Romania were: Italy (47), Cyprus and the United Kingdom (35), Australia (30), Germany and the USA (28).

The volume of external financial flows in 2020 presented by the NBR showed that:

- the most important countries that transferred money to Romania were: the United Kingdom (146,920,631,185 Euros), France (60,542,304,446 Euros), Germany (37,328,559,958 Euros) and Italy (35,235,149,432 Euros);
- the most important countries to which transfers were made from Romania were: the United Kingdom (133,035,838,975 Euros), France (68,152,450,087 Euros), Germany (23,734,822,972 Euros) and the Netherlands (23,638,587,721 Euros).

Corroborating the data on information requests sent/received by NOPCML with the volume of external financial flows, it can be seen that the states that send the highest number of information requests are the states that transfer high value amounts to Romania. So it follows that the participants in the information exchange are aware of the risk of money laundering involved in cross-border transfers and take all necessary measures to identify the origin of the money being transferred/received.

The typology related to transit accounts

The development of financial circuits involving companies registered in Romania, based in a law firm, with non-resident shareholders/directors/associates. The sums involved in the transactions were transferred from abroad and were followed (as soon as they were received in Romanian accounts) by transfers initiated to other non-resident companies registered in "off-shore" jurisdictions. An important feature of the transactions carried out according to the pattern is the use of the bank accounts of the companies involved, as transit accounts, without identifying an economic purpose for the respective financial transactions. Thus, the accounts opened on the territory of Romania were used as transit accounts, and the financial operations were carried out exclusively through Internet Banking. Another feature of this typology is the use of bank accounts in different jurisdictions. Following the requests for information prepared and the answers received, it turned out that the money transferred to Romania came from crimes committed on the territory of the state from where the money was originally transferred.

Specific threats of cross-border crimes

Cross-border transfers are used by criminals to legally transfer illicit proceeds.

Vulnerabilities:

- the transfer of proceeds of crime from one country to another by means of false documents;
- the use of internet banking and electronic transfers to make transfers characterized by speed and near anonymity;
- money obtained from a crime could be used to transit accounts to another country and then be re-transferred to a third country to hide the origin of the money;
- the process of obtaining information on foreign money involves time and money for the various state authorities, which means limited resources.

No.	Elements	Probability assessment (IT)	Assessment of consequences (C)	Risk rating
	Cross-border risk	**Average**	**Major**	**High**
Associated vulnerabilities: **Use of cross-border transfers** **Use of the foreign investment regime**				
Associated threat: **Investing or transiting the proceeds of crime**				
Event description: **Use of accounts opened by foreign citizens;** **The use of accounts opened by Romanian companies constituted by foreign citizens**				
Risk description: ***It's a high risk*** ***Average probability*** ***The consequences are major***				

Conclusion - the cross-border risk is classified as a high risk because the collection of data on the origin of the money that was transferred to Romania is a long and expensive process, and most of the time the money transits only the accounts opened in Romania.

From the ML/TF point of view, the process of globalization allows the easy transfer of money to different regions of the world, which increases the possibility of using such operations to hide funds of illicit origin. In addition, criminal networks operate in several countries to reduce the chances of being discovered, the use of multiple jurisdictions (including offshore jurisdictions) limits/reduces the efforts of the authorities to discover the perpetrators of the crimes.

The risk of financing terrorism through cross-border transfers is low because it is assumed that the money was transferred to Romania through financial institutions and remained in Romania or was transferred abroad and under such conditions was under bank control, and this channel is avoided by terrorists. Taking into account the fact that most of the time bank accounts were used strictly for the transit of money, these amounts were not externalized from the banking system and were under the control of these institutions.

5.2 Trade-free zones (also known as free zones) are an important tool in the globalization process, they are a customs agreement widely used around the world to facilitate trade.

Free zones are a type of special economic zone, an area where commercial legislation differs from that of the rest of the country. In a free zone goods can be unloaded, stored, handled, manufactured or reconfigured and re-exported under specific customs regulations and generally without being subject to customs duties. Free zones are normally organized around major seaports, international airports and national borders – areas with numerous geographical and commercial advantages.

In the free zones, a special regime of fiscal measures is applied, which make any form of illegal activity attractive, especially for predicate crimes.

In 2019, the World Customs Organization (WCO) conducted a study on 626 seizures, the study referred to the period January 2011-August 2018, it shows that drugs, counterfeit products, tobacco and weapons represented 23.5%, 22.8%, 9.9% and 2.7% of total seizures, respectively[145]. Organized crime groups (OCGs) that misuse free zones are often involved in numerous crimes, e.g. intellectual property rights offences, VAT fraud, corruption and money laundering.

Free zones in Romania are regulated by Law no. 84/1992 regarding the regime of the free trade zone and is applied by the Ministry of Finance through the Romanian Customs Authority.

In Romania there are six free trade zones, as follows: Constanta, Braila, Galati, Sulina, Giurgiu and Curtici - Arad.

In the category of potential vulnerabilities characteristic of the regime applied in free zones, are included:
- failure to declare goods when entering the free zone,
- non-declaration of goods when leaving the free zone,

[145]World Customs Organization, The "Extraterritoriality" of Free Zones: The Necessity for Enhanced Customs Involvement", Document of research no. 47 of OMV, available to Address: http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/research/research-paperseries/47_free_zones_customs_involvement_omi_en.pdf?la=en

- theft of goods stored in the free zone,
- incorrect declaration of goods at the time of unloading and storage in the free zone,
- non-declaration of amounts in foreign currency by foreign seafaring personnel on board ships berthed at port berths located in the free zone, as well as - corruption.

The generating actions for obtaining illicit funds that support money laundering are those of smuggling, i.e. the illegal introduction of high-risk goods (excisable products - cigarettes/tobacco, weapons, ammunition, drugs) and presentation/use of falsified documents at the customs authority.

Considering the activities supervised by the South Constanța customs office and carried out in the South Constanța Free Zone, South Port Constanța sector, it was found that control and monitoring measures are implemented, in order to reduce vulnerabilities in terms of generating actions, considering that:

- the placing of goods under the free zone regime, namely the introduction, storage, processing, transformation, sale of non-Union goods in the free zone, removal of goods from the free zone, are strictly monitored, controlled, supervised by BVF Constanta Sud;
- all building constructions in the southern sector were carried out with the prior consent for carrying out the activity of storing non-Union goods, of en-retail sales of energy products (fuel-diesel) with excise duty paid/Union customs status, of establishing a canteen where only canteens are consumed union products etc.
- the storage of goods in the free zone is carried out only in rented premises/land, assigned through APMC Constanta, only by free zone operators authorized by BV, i.e. by 36 Romanian companies with good standing. Of these, the operators who have no associates from Romania and who have leased/assigned the objectives for a period of more than 25 years stand out.
- in the area of territorial competence of the customs office/Sector South Port Constanta no operations/activities of the nature of the organization of exhibitions, stock exchange and financial-banking operations, sales of works of art are carried out.

Among the crimes detected at the level of the Constanța Sud border customs office, when removing the goods from the free zone, were:

- *submitting false documents to the customs authority*;
- *cigarette smuggling;*
- *drug smuggling.*

Offenses detected during the introduction/removal of goods in the free zone are also the introduction/removal of waste, provided for in art. 271 of Law 86/2006, art. 26 of Law 84/1992, art. 4 of Law 101/2011 in conjunction with art. 2 point 35 of REG. CEE. NO. 1013/2016, as follows:

- illegal introduction of waste through erroneous declaration regarding the type of goods declared/inscribed in the transport and T2L documents, respectively "used household items and used electrical appliances", instead of waste;
- illegal introduction of waste through erroneous declaration regarding the type of goods declared/inscribed in the transport documents and T2L, respectively "used tires", instead of waste;

At the level of the Giurgiu Free Zone Border Customs Office, a single case of crime was the detention of goods belonging to a commercial company, with a Turkish citizen as administrator, goods arrived from the USA and destined for the Arab Emirates, creating the suspicion of a violation of international sanctions.

The customs office only monitors the cash that crosses the border, declared by seafaring personnel who embark/disembark on maritime vessels that cross the border and who have the obligation to declare amounts exceeding 10,000 Euros, according to the provisions of REG.UE.1672/2018 regarding the control of cash that enters or leaves the Union and repealing Regulation 1889/2005, for which there is a reporting procedure.

Also, in the case of cash used for the payment of customs duties due, the provisions of Law no. 70/2015 of April 2nd, 2015 for strengthening financial discipline regarding cash receipts and payments and for amending and supplementing Government Emergency Ordinance no. 193/2002 on the introduction of modern payment systems.

Cash monitoring for amounts that are equal to or exceed the equivalent of 10,000 euros/person, found on seafaring personnel upon entering and exiting the free zone is carried out by submitting a written declaration, during the period January 1st, 2020-December 31st, 2020, a number of 15 declarations with a total value of EUR 324,381.89, and in the period January 1st, 2021-March 7th, 2021, a number of 3 declarations with a total value of EUR 65,931.15.

The border customs office of the Giurgiu free zone does not have any other data regarding the use of cash in this free zone as a result of the fact that natural persons are not allowed to enter this zone. The Giurgiu free zone is organized only for legal entities in this field. The Curtici Free Zone Border Customs Office is in the same situation.

Free Zones - specific threats

Free zones could be used by organized crime groups interested in smuggling and counterfeiting products. Also, free zones can be used to commit the crime of tax evasion, especially by avoiding payments to the state budget, by illegally using the tax facilities granted in the zone.

A specific situation of the free zones in Romania is their use for the illegal trade in tobacco and for the illegal introduction of waste through the erroneous declaration of the type of goods declared/inscribed in the transport documents.

Vulnerabilities:

- the storage of proceeds of crime, especially works of art, precious stones and metals, which are technically in transit so that they cannot be easily detected;
- the value of goods stored in free zones is established on the basis of the self-responsibility declaration and, in most cases, is not verified by the authorities;
- corruption of officials;
- the anonymity ensured by the procedure applied in the free zones.

No.	Elements	Probability assessment (IT)	Assessment of consequences (C)	Risk rating
	The risk related to	**Average**	**Minor**	**Low**

	Areas of Free Exchange			
Associated vulnerabilities: **Use of the special regime of free zones; Using a corrupt public official; Inadequate controls carried out by the authorities; Lack of cross-checking of the affidavit.**				
Associated threat: **Smuggling**				
Event description: **Use of cash transactions; Involvement of civil servants.**				
Risk description: ***It is low risk*** ***Average probability*** ***The consequences are minor***				

Conclusion- in Romania, the free zones are exposed to a low risk as a result of the strict control and the restrictive regime applicable in these zones.

The risk of financing terrorism through the use of free zones in Romania is low because cash is not used in this area, and the surveillance system is strict. Moreover, there is strict security of the area. The area is not accessible to the general public, being strictly supervised from the point of view of goods and people who have access to the area.

VI. TERRORIST RISKS AND FINANCING OF TERRORISM

Background analysis

6.1.1. Romania is located in Central and South-Eastern Europe, in the north of the Balkan Peninsula and has borders with the Republic of Moldova (NE and E), the Ukraine (N and E), Bulgaria (S), Serbia (SW), Hungary (W). It is one of the six riparian countries of the Black Sea (SE), with a coastal region with a total length of 225 km. Romania has the longest external border of the EU, and its geostrategic position requires ensuring a different level of border control, in accordance with Schengen standards and the provisions of the National Strategy for Integrated Border Management.

In recent years, the pressure of illegal migration at Romania's borders has increased, especially at the borders with Serbia and Hungary, our country being a transit area towards Western Europe. Illegal migration at Romania's borders (with entry from Serbia and Bulgaria and exit to Hungary) will continue to be influenced by the migration flow from the Western Balkans and from the subsidiary route, from Central Asia, South Asia and the Middle East.

People with a radical profile were identified, whose extremist options are mainly manifested in their speech and attitude (praise of terrorist organizations, threats, incitement to violence, aggressive behavior, rejection of state authority, etc.), without visible intentions to act on the line committing a terrorist attack. Among these persons are persons convicted by the court, pursuant to Law no. 535/2004 on the prevention and combating of terrorism, as a result of the activities carried out mainly as a result of the systematic promotion of terrorist propaganda messages/materials.

6.1.2. Romania is not a financial and banking center or an important commercial center, and by Law no. 70/2015 meant to strengthen financial discipline in terms of cash receipts and payments operations, the maximum value of cash payments was limited. However, the incidence of cash payments remains high.

In terms of threats, given the different nature of the crimes, money laundering and terrorist financing are usually assessed separately. In terms of vulnerabilities, although the purpose and nature of ML and TF may be different, criminals often use similar techniques to transfer illegal money or try to exploit the same vulnerabilities.

By Law no. 58 of April 8, 2019 for the amendment and completion of Law no. 535/2004, the provisions of Directive (EU) 2017/541 on combating terrorism have been transposed into national legislation. Through this legislative amendment, the definitions related to "funds" and the "terrorist financing crime" were amended, and the area of activities assimilated to acts of terrorism was expanded, the financing crime[146] *of terrorism being included in this category.*

- the crime of financing terrorism sanctions the financing of terrorist acts, the financing of a terrorist entity or a person involved in terrorist activities, with the intention of using them or knowing that they are to be used for these purposes;
- the scope of assets that can be the subject of the crime of financing terrorism has been expanded by redefining the concept of "funds", which represents "goods of any nature, tangible or intangible, movable or immovable, acquired by any means and legal documents or instruments in any form, including electronic or digital form, evidencing ownership or an interest in such goods, bank credits, traveler's cheques, bank cheques, warrants, shares, securities, bonds, special drawing rights and letters of credit, without this enumeration being limiting." (art. 4 point 8 of Law no. 535/2004);
- all crimes mentioned in Law no. 535/2004 are acts of terrorism (for example, financing terrorism, directly involving or supporting in any way the commission of a terrorist attack/terrorist entity, repeated access to terrorist propaganda materials or their possession for the purpose of appropriating terrorist ideology, as part of a process of radicalization, movement of a person for terrorist purposes, etc.).

6.2. Contextual Threat Analysis (Terrorism)

6.2.1. This criminal phenomenon remains very low in Romania. Also, according to the European Union report on terrorism and the latest trends, published in 2021, the number of terrorist attacks registered in the EU remained stable compared to the last two years, when a decrease in this criminal phenomenon was observed compared to the period before 2019.

Regarding terrorism, in December 2020 the European Union adopted the EU Counter-Terrorism Agenda: Anticipation, Prevention, Protection and Response Capacity. The EU agenda includes preventing and combating the financing of terrorism.

In line with the EU Security Strategy adopted in December 2020, international cooperation is also essential to eliminate all sources of terrorist financing, for example cooperation within the Financial Action Task Force. The Strategy also underlines that the growing trade in cultural goods has become one of the most lucrative criminal activities, a source of funding for both terrorists and organized crime. According to the strategy, ways to improve the online

[146] According to art. 36 of Law no. 535/2004

and offline traceability of cultural goods should be explored, as well as possibilities to actively support law enforcement authorities and academia.

(1) The offence of financing terrorism shall be punishable by imprisonment for a term of 5 to 12 years and disqualification from exercising certain rights if funds, whether lawful or unlawful, are collected or made available, directly or indirectly, with the intention that they should be used or with the knowledge that they are to be used, in whole or in part, for the commission of terrorist acts or for the support of a terrorist entity.
(2) The commission of an offence for the purpose of obtaining funds with the intention that they shall be used or with the knowledge that they are to be used, in whole or in part, for the commission of terrorist acts or for the support of a terrorist entity shall be punishable by the penalty prescribed by law for that offence, the maximum of which shall be increased by 3 years.
(3) If the funds obtained under the terms of paragraph 1 are used for the commission of a criminal offence, the offender shall be liable to a fine of (2) were made available to the terrorist entity, the rules on concurrence of offences shall apply.

6.2.2. The prevention of terrorism is a priority area at the national level; thus, one of the national security objectives highlighted in the National Defense Strategy 2020-2024 is the prevention and combating of terrorist risks associated with the activities of specific organizations, the presence on the national territory of members or followers of such entities, the intensification of extremist jihadist propaganda, in especially in the online environment, as well as radicalization processes[147] from Romania.

Currently, the current level of terrorist alert in Romania is "Cautious", the second level on a scale of four (1. Low; 2. Cautious; 3. High; 4. Critical), according to the National Terrorist Alert System, approved by The Supreme Council of National Defense. We specify that the "Cautious" level is established and maintained as long as, at the national level, there is a risk of a terrorist act, but the probability of its occurrence is low.

6.2.3. In our country there are no internal conflicts of a political, religious or social nature that could be a catalyst for terrorist activities. Also, our country is not facing a domestic terrorist phenomenon. Terrorist risks are closely linked to developments in external areas, particularly terrorist attacks in Europe and security crises in MENA[148] and Afghanistan – Pakistan. Romania is not subject to a direct/concrete and consistent threat from a certain terrorist entity.

The radicalization generated and fueled by pro-Daesh propaganda, skillfully combining a radical interpretation of the Islamic religion with the organization's political goals, has come to represent an important internal source of risk and a major security concern.

Another way through which profile risks infect the national territory is migration in connection with terrorism, given that our country is placed on several routes on the MENA/Afghanistan-Pakistan-Europe relationship.

6.2.4. No terrorist organization or cell is active in Romania and we have not faced any terrorist attacks in our country. We do not exclude the possibility of a terrorist attack on the national territory, but the probability of a terrorist attack is low.

[147]The complex process by which a person comes to pervert their beliefs, feelings and behavior, as a result of adopting an extremist way of thinking, in which the use of violence and even self-sacrifice through suicidal methods are legitimate and desirable forms of defense and/or satisfaction of interests promoted by terrorist entities. [Article 4 paragraph (27) of Law no. 535/2004]
[148] Middle East and North Africa

In addition, there are no indications of the establishment in Romania of organized crime networks that are involved in criminal-terrorist hybrid actions.

Romania faced an isolated number of cases, in which Romanian citizens or foreigners residing in our country were convicted for their involvement in activities that consisted of: (1) terrorist propaganda, carried out especially in the online environment; (2) accessing repeated transmission of terrorist propaganda materials, through computer systems or other electronic means of communication, as well as possession of such materials, with the aim of appropriating terrorist ideology, as part of a radicalization process; (3) receiving or obtaining instructions by self-documentation regarding the manufacture or use of explosives, firearms or any other weapons, noxious or dangerous substances or regarding specific techniques or methods of committing or supporting the commission of a terrorist act.

The analysis carried out regarding the means by which the activities were carried out highlighted the fact that they were carried out using their own resources (laptop, telephone, internet connection). This type of activity does not involve a considerable financial effort, being accessible to everyone.

6.2.5. The main terrorist organizations considered to pose a terrorist threat internationally are Daesh and Al-Qaeda, terrorist organizations with global reach, especially in terms of the pool of sympathizers and groups subordinate/affiliated to their ideology. Since 2015, with the rise of the Daesh terrorist organization and the increase in propaganda activity online attacks initiated by sympathizers of the jihadist entity have highlighted a new modus operandi in terms of preparing and committing a terrorist attack. The main defining element of today's terrorist actions is based on provoking casualties and creating a general sense of panic with minimal preparation, using logistical elements that are readily available / affordable to anyone and at low cost.

Also, some terrorist organizations act armed only locally, but fund-raising activities are carried out internationally.

6.2.6. As a rule, terrorist organizations need most of their financial resources to create and maintain their organizational structures (such as creating organizational logistics and for propaganda). Instead, in many cases only small amounts are needed to carry out actual attacks.

The costs of committing a terrorist attack depend on the means and methods used by the perpetrators, such as:

- in the case of a terrorist attack by a radicalized person acting spontaneously, the related cost is that of buying a knife or renting a vehicle that he can use to drive into a crowd;
- In the event of an organized and planned terrorist attack, the cost could be high and variable. According to www.osce.org, the cost of the terrorist attack on the USS Cole (2000) was between $5,000 and $10,000, while the cost of the 9/11 terrorist attack (2001) was over $500,000.

6.2.7. Romania – transit zone between Western Europe and areas that generate terrorist risks.

Romania continues to be exposed to illegal migration, with the perpetuation of risks to national security, including those of a terrorist nature. The main security risks in the area of counter-terrorism stem from the possibility of access to the national territory of persons undergoing (self-)radicalization or associated in any way with terrorist/extremist entities.

We specify that, in accordance with the National Defense Strategy 2020-2024, a major trend with the potential to affect and influence the security environment, in the perspective of 2024, is the fact that migration flows from the Middle East, North Africa, Afghanistan and Pakistan will continue to target Romania as a secondary transit route to Western Europe, which could be used by individuals with links to terrorist/extremist organizations to enter the national territory.

In assessing the terrorist threat represented by migration-related issues, the authorities consider two constant coordinates that characterize Romania's profile in this field:

- the predominant nature of transit and temporary station space for migrants (originating/MENA, Sub-Saharan Africa and Afghanistan-Pakistan) moving to Western Europe. At the national level, the pressure of the migration flow is mainly manifested at the Romanian-Serbian border, in the context where our country is a transit area (on the Balkan sub-route) to Europe;
- the location of Romania on a secondary route of illegal migration flows with the destination of Western Europe - the western space thus remains the main destination for illegal migrant flows.

On the other hand, the risk factors in this segment have a strong exogenous character, depending directly on the developments in the areas of origin of the migrants, states affected by security crises and instability, particularly in MENA.

Regarding the general trend at the EU's external borders, in 2020 the restrictions imposed in the context of the health crisis caused by the COVID-19 pandemic led to a decrease in migration flows. The Western Balkans remain the main transit area for migratory flows bound for the Schengen Area, the end of 2020 marking an intensification of the phenomenon of illegal migration on the Balkan sub-route.
In the next period, migration flows may fluctuate depending on the evolution of the security situation in this region (a possible deterioration being likely to fuel the migration flows that access the European continent).
In accordance with the evolution of the phenomenon at the European level, the competent national authorities keep in mind the problem of illegal migration, including from the perspective of connections with terrorism, calibrating their efforts to prevent and combat terrorism and radicalization, focused on the preventive dimension.

6.2.8. Romania's potential transit role for foreign/returned terrorist fighters (FTF/R).

FTF and Returnees (foreign terrorist fighters) represent one of the main terrorist threats to Europe. The national authorities with responsibilities in the field of preventing and combating terrorism, and whose general approach is eminently preventive, carefully monitor the persons falling into the categories of FTF and Returnees (foreign terrorist fighters), in order to prevent the materialization of risks to national security.

There have been no registered cases of Romanian citizens / residents in our country leaving the territory of Romania to join terrorist organizations / jihadist entities. No Daesh actions of recruiting combatants were identified - from Romania or carried out on the territory of our country, the option of joining terrorist entities being exclusively the prerogative of a general propaganda, carried out in the virtual environment.

Until now, the migration flow has not influenced the level of terrorist risk in Romania, and our country was not an option for migrants as a destination state. However, the maintenance of migratory pressure from Syria-Iraq, Afghanistan-Pakistan and North Africa fuels the risk that among the people transiting the national territory are also members or supporters of terrorist/jihadist entities.

The threat generated by members or supporters of terrorist/jihadist entities accessing the migration flow can be:

- direct, immediate and planned (eg involvement in the execution of a terrorist attack);
- latent and with multiple developments, amplifying the risks from a national level (propaganda, radicalization, the establishment of logistical, financial and/or operational support points).

The major risk faced by former foreign terrorist fighters returned from conflict areas is that of subsequent reactivation not only in the country of origin, but also on the territory of other Eastern European states, including Romania.

6.2.9. Radicalization in Romania is not manifested at the level of a phenomenon, but in the form of isolated cases, subscribed to the radical-Islamic ideology.
These are found especially among foreigners originating from states with terrorist problems, but also among Romanian citizens who have converted to an erroneous/perverted form of Islam. In most situations, radicalization occurs on a vulnerable background of the individual.

In general, in Romania, people in different stages of the (self-)radicalization process manifest themselves exclusively in a discursive or behavioral register, without concrete steps to move to the action part being identified.

As a result of the impact of the propaganda and jihadist actions of Daesh, promoted online, in recent years we have seen in our country an upward trend in cases of (self) radicalization among Romanian citizens converted to Islam, including in the youth segment, but which until now it did not reach manifestations of the magnitude of a phenomenon.

Propaganda actions in favor of terrorist/jihadist entities undertaken by Romanian citizens or foreign citizens living in our country are only individual and uncoordinated initiatives, caused by the radicalization processes they go through. The Internet remains the primary medium for accessing and disseminating terrorist propaganda and radical-jihadist messages, while also facilitating connections with other radicalized individuals.

In the cases where terrorist propaganda activities represented the offense provided for in Article 33^2 paragraph (4) of Law no. 535/2004, the High Court of Cassation and Justice of Romania ordered the sentencing of the persons in question to custodial sentences for their

involvement in activities of systematic promotion of radical ideas, beliefs or doctrines, with the intention of instigating the commission of a terrorist act.

6.2.9.1 *The national penitentiary system* does not face a case law and intensity of radicalization at the level of a phenomenon. In Romanian penitentiaries, there have been isolated cases of convicted persons going through a process of radicalization, these being both among persons convicted of crimes circumscribed to acts of terrorism, and of those convicted of committing common law crimes.

The case study at the European level highlights the need for sustained cooperation on this issue both between the institutions responsible for ensuring national security, and between them and civil society. Such an approach, under development also in Romania, must have as its objectives both the early identification and assessment of security risks, as well as the practical implementation of a process of reintegration of the prisoner, initiated from the period of detention and continued after release, aimed at to alter the process of radicalization to the point of abandoning the option for violence.

6.2.9.2. In Romania, the radicalization process is triggered mainly in the online environment, by establishing contact with elements affiliated with ideologies or terrorist/extremist entities and accessing jihadist propaganda materials.

The online environment is mainly represented by social media platforms, chat-games, games, forums, jihadist websites. Unlike classic communication media, the virtual one presents a series of advantages for radicalizing elements such as: the speed of message transmission, the anonymization offered by certain platforms, the possibility of encrypting the disseminated elements / discussions, the ease of accessing the message, the possibility of choosing the target audience, etc. People who go through a process of radicalization on the internet stand out by:

- persistent viewing of jihadist/terrorist propaganda materials and downloading them for dissemination on personal accounts open on social media platforms/messaging applications;
- activities promoting radical ideology and supporting jihad, respectively terrorist entities/radical imams, through social networks.

6.3. Analysis of the threat posed by terrorist financing

6.3.1. General aspects

Access to consistent and constant sources of financing is vital for the existence and functioning of terrorist organizations and the diversity of sources of income and the possibilities of their conspiracy constitute major challenges in countering terrorist financing activities.

The idea that terrorism as a whole does not require significant costs to finance is wrong. The financing of terrorism is different from the financing of a single terrorist act because some terrorist organizations need funds to operate as complex structures (a relevant example is the terrorist organization Al Qaeda, which created the paradigm of the network terrorist organization, with a center and local franchises).

Thus, terrorist organizations need funds for: recruitment (propaganda, supporting the activities of recruiters, etc.); training facilities, including people to ensure the training steps; accommodation, food (including for sleeping cells); equipment, weapons, explosives; identity documents and travel expenses; communications; gathering information; post-operational expenses (for example, to support the relatives of the attackers).

The situation is different outside of conflict zones, in places like Europe, where followers of terrorist entities often do not need significant material support. The sums needed to plan and execute attacks similar to those of recent years - carried out by singular actors, with rudimentary, simple means - do not require special financial efforts; even the organization of larger actions is unlikely to exceed the material possibilities of an individual or a small group.

Terrorist attacks that caused panic in Europe were carried out, in most cases, by using white vehicles and weapons in very crowded urban places, resulting in a high number of victims, creating a general feeling of panic / insecurity without significant costs.

There are multiple taxonomies of the means of financing terrorism, but most specialists distinguish four main sources of financing, namely:

- *state funding* - in this case, the financing is provided by states, known as sponsor states, being generally listed at international level and usually subject to political and economic restrictions, sanctions or constraints, imposed by the international community;
- *carrying out illegal activities* - generally through activities specific to organized crime. It is one of the most popular methods, because it leads to obtaining large sums relatively easily, but it also presents considerable disadvantages. The range of illegal activities is very diverse: narco-terrorism, cigarette and diamond trafficking, piracy, kidnappings, counterfeiting of various forms, robberies, imposition of "taxes", credit card fraud, money laundering, extortion, etc.
  Cooperation between organized crime and terrorism actors can include long- or short-term agreements, typically used to gain experience or operational support. There may still be situations in which organized crime networks resort to terrorist tactics, exclusively to secure and protect their operational-criminal environment. In the case of terrorist organizations, the main reason why they usually get involved in criminal operations specific to organized crime is self-financing;
- *carrying out legal activities* - by initiating legal affairs, by the terrorist organizations themselves or through front persons and organizations. The economic fields in which these businesses can be carried out are very diverse: trade, investments, production of various goods, construction companies, transactions with energy resources, restaurants, clubs, security companies, transport services, etc.;
- *popular support* - represents the financing of the terrorist organization by a larger number of people, generally with small amounts, being an indicator of the population's perception of the legitimacy of a terrorist group.

Analysis of the data obtained (from open sources, expert opinions, international case studies, etc.), including from cooperation with other States, has revealed that terrorist organizations worldwide exploit various means of collecting and transferring funds, which ensure that transactions are not monitored by the authorities, that they are anonymized and that the real

beneficiary is not identified, i.e.: (1) complex financial channels; (2)[149] the hawala system; (3) virtual assets/cryptocurrencies[150]; or (4) the physical transport of cash; the cross-border transport of cash below the threshold of EUR 10,000.
In Romania, no cases of terrorist financing have been identified through the use of these instruments, and there are no networks established at the national level that operate for this purpose. However, the Romanian authorities are aware of the threats posed by the use of such instruments for the purpose of financing terrorism and carry out activities aimed at identifying such situations.

6.3.2. In this context, the sector supervised by the NBR has a solid compliance culture, the risks identified being related to indirect control, correspondent accounts and trade finance.

In order to identify such risks, within the inspections carried out by the NBR, high-risk transfers are analyzed and the scenarios implemented for transaction monitoring are evaluated, the way in which the parameters are established within the screening application and effective detection tests are carried out in order to ensure that the scenarios are adapted to the client portfolio and the type of financial institution assessed.

In addition, the NBR uses other types of risk monitoring tools, such as periodic questionnaires sent to supervised institutions, to collect quantitative and qualitative information that highlights the potential vulnerabilities of some processes or lines of activity, including in terms of implemented scenarios for signaling risks.

Simultaneously with the supervision and monitoring activities, to support the reporting entities in fulfilling their legal obligations, the NBR sends risk awareness letters to the supervised sector.

Also, particular importance is given to international CTF guidelines, with the NBR requesting supervised entities to take the necessary measures, from the perspective of ensuring adequate management of potential risks, for example in relation to: Virtual Assets and Virtual Asset Service Providers[151]; Guidance on Terrorist Financing Risk Assessment[152]; Virtual Currencies and Terrorist Financing: Assessing Risks and Evaluating Responses[153]; Financing Terrorist Recruitment[154]; Best Practices on Combating Misuse of Non-Profit Organizations[155]; Guidance on Criminalizing Terrorist Financing[156]; International Best Practices: Targeted financial sanctions related to terrorism and terrorist financing

[149]The method works by transferring money without actually moving it. Hawala schemes are widespread throughout the world, particularly in the Middle East, North Africa and the Indian sub-continent. Money is transferred between hawala systems in exchange for a variable fee paid by the beneficiary. In terms of source of funds, the system comprises White Hawala - where the money comes from a legal source, and Black Hawala - where the money comes from an illicit source.
[150] They make it possible to use them for operational purposes, including obtaining funds for terrorist attacks resulting in security risks. Cryptocurrencies have become increasingly tempting for terrorist entities due to the advantages they offer, namely the lack of traceability of transactions and the high degree of anonymity of financial transactions. These aspects lead to the creation of a viable financial mechanism, which can avoid both the financial sanctions imposed on terrorist entities and the risks of identifying the persons involved and the entire financial circuit.
[151] https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-will-VASP.pdf
[152]https://www.fatf-gafi.org/publications/methodsandtrends/documents/terrorist-financing-risk-assessmentguidance.html
[153] https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf
[154] http://www.fatf-gafi.org/publications/methodsandtrends/documents/financing-recruitment-terrorist-purposes.html
[155] http://www.fatf-gafi.org/publications/financialinclusionandnpoissues/documents/bpp-fighting-abuse-npo.html
[156] http://www.fatf-gafi.org/publications/fatfrecommendations/documents/criminalising-terrorist-financing.html

(Recommendation 6)[157]; The role of Hawala and other similar service providers in money laundering and terrorist financing[158]; Report from the Commission to the European Parliament and the Council on assessing the risk of money laundering and terrorist financing affecting the internal market and on cross-border activities[159] and further guidance on the implementation of international sanctions in this report).

The risk associated with cross-border exposure remains relevant, but not as important as in the case of Member States recognized as international financial centers.

The most important risk factors related to cross-border activities are represented by the geographical areas and the customers involved in the transactional flow.

In terms of geographical risk, namely high-risk third countries with strategic deficiencies[160] (HRTC), the total volume of transactions involving these jurisdictions represents 4.19% of the total volume of cross-border transactions carried out by banks in 2020 (2.39% of the volume of receipts and 6.46% of the volume of payments) and 0.58% of the total volume of cross-border transactions carried out by accessing money remittance services (via MVTs) in 2020 (0.36% of the volume of receipts and 2.74% of the volume of payments). For this estimate, HRTCs that were reported by the FATF later in 2021 were taken into account, although they were not on the FATF list of monitored jurisdictions at the time of the transactions in 2020.

During 2020, NOPCML received approximately 402 STRs regarding operations or persons in relation to high-risk third countries that have strategic deficiencies, of which 86.82% were submitted by banks, and 12, 44% of MVTS. About 64% of these STRs received by NOPCML concerned individuals who had nationality in these jurisdictions, 31% concerned transactions with those jurisdictions, and 2% concerned legal entities. In addition, 3 STR were submitted by public notaries and involved participants in transactions of foreign nationality, respectively from high-risk third countries.
Considering the figures mentioned above, we conclude that awareness of the TF/FP risk is high, especially in the financial sector.

In addition, in 2020, NOPCML received 3 requests for information on certain aspects related to the financing of terrorism, which were immediately resolved.

The correct application of standard and supplementary know-your-customer measures (CDD/EDD) is a primary step to prevent the misuse of the financial system by criminals, and the NBR continuously monitors, through demanding checks of internal procedures and their implementation, compliance with the provisions of Law no. 129/2019, as amended and supplemented, which is the legal act transposing Directive (EU) 2015/849, as amended and supplemented, compliance with the provisions of Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No. 1781/2006, as well as compliance with guidelines (EBA etc.) and best practices (FATF/FATF - MONEYVAL etc.). According to them,

[157] http://www.fatf-gafi.org/publications/fatfrecommendations/documents/bpp-finsanctions-tf-r6.html
[158] https://www.fatf-gafi.org/media/fatf/documents/reports/Role-of-hawala-and-like-in the-ml-tf).pdf
[159] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019SC0650&from=EN
[160] Delegated Regulation (EU) 2016/1675of the Commission of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries that have strategic deficiencies, as amended:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R167520210207

financial institutions apply know-your-customer (standard/supplementary) measures proportionate to the money laundering and terrorist financing risk they have identified and do not establish a business relationship if they are unable to comply with these requirements, if they have not ensured that the purpose and nature of the business relationship is legitimate or that they can effectively manage the risk of being used for money laundering or terrorist financing purposes.

In this context, supporting documents of high-risk transactions are a mitigating factor.

- Lista GAFI a jurisdicțiilor cu risc ridicat care fac obiectul unui apel la acțiune (FATF list of High-Risk Jurisdictions subject to a Call for Action): http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-february-2020.html
- Jurisdicții care fac obiectul monitorizării sporite (Jurisdictions under Increased Monitoring) – 21 februarie 2020: http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-february-2020.html
- Jurisdicții GAFI supuse monitorizării sporite (FATF Jurisdictions under Increased Monitoring) – iunie 2021: http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-june-2021.html

In addition, current accounts can be used for terrorist financing purposes, especially for low-volume transactions.

Correspondent banks carry an inherently high risk due to complex international interconnections, with the potential to be frequently used as a means of disguising payments to high-risk jurisdictions. However, during the analyzed period, there were no cases of closed correspondent relationships due to repeated provision of funds transfers with incomplete/missing mandatory data.

Thus, regarding the risks of current accounts and correspondent relationships, financial institutions have the obligation to segment, customize and permanently update the scenarios/limits implemented for pre- and post-transaction monitoring, to ensure a dynamic process of continuous monitoring of customer operations.

Certain vulnerabilities in indirect control, which are more difficult to detect, could be related to the failure to implement early warning mechanisms regarding the risk circumstances aimed at the dynamics with which commercial companies (for example, newly established) changes its shareholding structure and management mandate (for example, shortly after the initiation of business relations), which could make it difficult to properly apply measures to identify and verify the identity of associates, administrators and beneficial owners, favoring opacity in what concerns the establishment of groups of companies, which could affect the process of assessing the risk profile and monitoring the business relationship.

Another relevant risk factor is the activity of money remittance services, which is also carried out by banks and which involves high risks, especially in the case of cash transactions with an international dimension and payments made outside an existing business relationship (occasional transactions below thresholds that legally require customer due diligence). In the case of remittances to high-risk jurisdictions, there is also the possibility that the payments may be used in connection with the financing of terrorism.

In particular, remittances through remittance service providers with an extensive network of agents globally present a significant level of money laundering and terrorist financing risk. The high level of risk is determined by the fact that money remittance services are frequently

used for money laundering and terrorist financing, being easily accessible without specific knowledge or prior planning. Money remittance service providers mostly rely on agents to run their business and thus agents are their main vulnerability.

As resilience/risk mitigation measures to improve the governance framework, policies, procedures and controls used for effective risk management, we maintain the implementation of demanding human resource management standards, as well as training sessions dedicated to the obligations on the CTF/CFP/international sanctions line, including awareness of the consequences of non-fulfilment of responsibilities and the implications for the institution and for the persons holding such duties through the job description, or who are responsible for non-compliance with legal provisions in case of incidents.

In this sense, the NBR issued letters of recommendation addressed to the institutions under its supervision.
A survey of financial sector entities identified the following main risks related to terrorist financing:

- the international climate (terrorist attacks in European cities, the situation in Syria, Iran, North Korea, Ukraine, the pronounced phenomenon of migration from the Middle East to European states, the situation in Afghanistan);
- persons/entities that issue/distribute and/or trade in any form electronic currency/virtual assets;
- fund transfer operations – as they can constitute a channel for the transfer of funds for the purpose of financing terrorism.

6.3.3. The Financial Supervisory Authority monitors[161] the implementation by supervised entities of the provisions of Law No 535/2004 on preventing and combating terrorism, and approves or rejects[162] authorizing a financial transaction between residents and non-residents, as well as between non-residents, consisting of current account or capital account operations carried out for or on behalf of natural or legal persons listed in the Annex to Government Emergency Ordinance No 159/2001 on preventing and combating the use of the financial and banking system to finance acts of terrorism, approved by Law No 466/2002, and refer the matter to the Prosecutor's Office of the High Court of Cassation and Justice - Directorate for the Investigation of Organized Crime and Terrorism, as well as to the Romanian Intelligence Service. At the same time, we mention CNVM Order No 9/2005 approving Instructions No 4/2005 on the prevention of terrorist financing, which covers the obligations of entities regarding prohibited operations, authorized operations and sanctions applicable in case of misconduct. On the basis of this Order, to date, the CNVM, and after the establishment of the FSA, has not applied any sanctions. On the basis of this order, to date, the CNVM and, since the establishment of the FSA, have not applied any sanctions.

According to Annex I of the FATF Guidance on Assessing the Risk of Money Laundering or Terrorist Financing at the National Level, terrorist financing risk factors are related to raising/collecting funds from criminal activities, i.e. NGOs, misleading use of "legal" funds (e.g. NGOs, donors unaware of the use of the financial fund), donations from legal income (e.g. salaries and profits), transfers of funds and/or using funds.

[161] Article 31 of Law no. no. 535/2004
[162] Article 28 of Law no. no. 535/2004

Reporting entities are required to identify, assess and mitigate the risk of terrorist financing and the supervision carried out by the FSA verifies the implementation of this obligation. The sample of transactions assessed in the course of supervisory actions includes all risk factors related to high-risk jurisdictions, high-risk customers (residence, nationality, travel to these jurisdictions or business relationships with individuals or legal entities/organizations in these jurisdictions, including publicly exposed persons), such as Afghanistan, Iraq, Syria, Iran and DPRK, or associates of a terrorist group, such as Al-Qaida, ISIL, Da'esh[163].

The supervisory activities also assess the monitoring of business relationships, check the parameterization of risk assessment tools, internal control systems, the use of an updated list of designated persons and the timely submission of the STR/FT report. The FSA has regularly sent out awareness letters on FT risks related to red flags, such as the use of entities that could be linked to terrorist activities or related persons, and during controls or based on requested follow-up reports on the implementation of action plans, the FSA verifies whether these measures have been implemented.

During 2017-2020, the FSA received no STRs related to terrorist financing risks (transaction with high-risk jurisdiction, non-commercial purpose of transaction, money sent frequently and received from HRTC, customer due diligence with a list for designated persons and entities).

At the same time, the FSA pays particular attention to transactions with atypical elements, such as jurisdictions for which there is a smaller inflow of transactions. The analysis covers terrorist financing risks in line with the risk matrix covering occasional transactions and business relationships. Most of these (including in terms of volume) are set on a contractual basis, such as reinsurance premiums, although none of them were subject to STR/TF.

In addition to on-site controls, as part of off-site supervision, the FSA uses other types of tools to monitor terrorist financing risks, including entity behavior, using questionnaires and regulated reports to collect quantitative and qualitative information to highlight potential internal process vulnerabilities that generate terrorist financing risks. In this regard, the FSA identified the following vulnerabilities during its controls:

- Weaknesses in meeting customer due diligence measures in relation to the customer and also the beneficial owner or controlling person due to non-transparent holding mechanism;
- Failure to carry out an adequate assessment of intermediaries (use of third parties) in relation to customer due diligence for anti-money laundering and anti-terrorist financing purposes;
- Failure to verify information collected by intermediaries directly from the client, relying solely on the customer due diligence measures carried out by the intermediary;
- Weaknesses in the oversight of trading activity in monitoring any suspicious activity for AML/CTF purposes;
- Lack of a money laundering or terrorist financing risk assessment or outdated money laundering or terrorist financing risk assessment; (FATF R1. C1.10);

[163]List of mentions in Council Implementing Regulation (EU) 2021/138 of 5 February 2021 on the implementation of Article 2(3) of Regulation (EC) no. 2580/2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism and repealing Implementing Regulation (EU) 2020/1128

- Lack of continuous monitoring of factors posing a high risk of money laundering or terrorist financing (taking into account volume of transactions, type of customer, product, service, distribution channel or geographical area);
- Insufficient resources to cover money laundering or terrorist financing obligations.

Terrorist financing risks associated with different types of customers revealed the following threats to which non-banking financial entities are exposed:

- Use of straw men or carriers in casual business dealings or transactions;
- Using a long/non-transparent chain of equity ownership to cover up indirect terrorist control;
- Using financial sectors to transport money to people close to terrorists.

Risk remediation measures for terrorist financing vulnerabilities are also taken, such as training courses, public list of designated persons, public warnings and direct communication with representatives of the management of financially supervised entities.

From TF's perspective, we assess a low degree of risk, both in terms of financial flows and products offered by non-banking financial institutions, and from a sector perspective.

6.3.4. Risk of terrorist financing in connection with possible violation, non-implementation or circumvention of targeted financial sanctions (TFS)

According to the FATF Guidelines/Guidelines, the risk of a potential breach or non-implementation of targeted financial sanctions (TFS) may materialize when designated entities and persons, due to inadequate screening procedures and a general lack of compliance culture, access financial services and/or funds or other assets, for example, delays in communicating designations at national level, lack of clear obligations for private sector entities, failure of private sector entities to adopt adequate policies and procedures to address risks (e.g. poor client acceptance and ongoing monitoring procedures and processes, lack of staff training, ineffective risk management procedures, lack of an adequate screening system, etc.). The risk of non-implementation of targeted financial sanctions is also related to and may materialize due to concerted efforts by designated persons and entities to circumvent international financial sanctions (e.g. through the use of shell or dummy companies, joint ventures, fictitious accounts, fraudulent/fictitious intermediaries and persons or entities acting for or on behalf of designated persons or entities).

In this sense, the threat refers to designated persons and entities that have previously caused or have the potential to circumvent, violate or exploit a past, present or future non-compliance with the implementation of the TFS. Persons or entities acting for or on behalf of designated persons or entities may also pose such a threat. As noted in the FATF Recommendations, not all threats pose the same level of risk to all countries, while the absence of cases involving known or suspected violations related to non-implementation or circumvention of the TFS in a particular country does not necessarily mean that a country or private sector firm is at low risk.

Designated persons and entities have used diverse and evolving methods to disguise illicit activities, and the networks they control deliberately spread their operations across multiple jurisdictions. Accordingly, countries and private sector firms should continue to consider the

likelihood of funds being made available directly or indirectly to these persons or entities in their jurisdictions or through customer relationships or the use of their products.

Sectoral vulnerabilities may refer to the weaknesses and contextual characteristics of a particular sector that lead to persons and entities designated to exploit it for the purpose of circumventing the TFS. Weaknesses such as a low level of risk awareness or understanding of TFS requirements and a general poor compliance culture within a sector are all vulnerabilities to misuse. However, based on experiences to date with money laundering/terrorist financing risk assessments, countries tend to place greater emphasis on the banking or money or value transfer sector, as designated persons and entities need access to the international financial system to process payments for components or materials from foreign sources, which often have direct financial links to high-risk jurisdictions, and less on non-bank financial entities.

General legal framework

Application of international sanctions in Romania:

- Government Emergency Ordinance no. 202/2008 on the implementation of international sanctions, approved with amendments by Law no. 217/2009, with subsequent amendments and additions;
- NBR Regulation no. 28/2009 on the supervision of the implementation of the international sanctions blocking funds, with subsequent additions;
- NBR Regulation no. 7/2011 regarding the modification, completion and repeal of some normative acts;
- NBR order no. 340/2010 regarding the unitary reporting model of funds and blocked economic resources;
- FSA Regulation no. 25/2020 on the supervision of the implementation of international sanctions by the Financial Supervision Authority.

Prevention of money laundering and terrorist financing:

- Law no. 129/2019 for the prevention and combating of money laundering and the financing of terrorism, as well as for the amendment and completion of some normative acts, with subsequent amendments and additions;
- NBR Regulation no. 2/2019 on preventing and combating money laundering and terrorist financing;
- FSA Regulation no. 13/2019 regarding the establishment of measures in the field of combating money laundering and the financing of terrorism through the financial sectors supervised by the Financial Supervisory Authority, with subsequent amendments;
- CNVM order no. 9/2005 regarding the approval of Instructions no. 4/2005 on the prevention of the financing of acts of terrorism;
- Regulation (EU) 2015/847 of the European Parliament and of the Council on information accompanying transfers of funds and repealing Regulation (EC) no. 1781/2006 (with direct applicability);
- EBA guidelines applicable to the prevention and combating of money laundering and terrorist financing.

In accordance with the provisions of Article 3 of GEO No 202/2008, the acts referred to in Article 1(1) of GEO No 202/2008 are binding in domestic law for all public authorities and institutions in Romania, as well as for natural or legal persons who are Romanian or located

on Romanian territory, under the terms of the regulations establishing the legal regime for each category of acts. The resolutions of the United Nations Security Council and the regulations and decisions of the European Union are directly applicable.

6.3.5. Implementation of specific financial sanctions in the sector supervised by the FSA

In the area of supervision of the application of the international sanctions regime for supervised sectors, the FSA has made available to entities alerts and best practice guides in this area to increase awareness and compliance through the dedicated section of the FSA website[164]. Supervised entities are kept informed on an ongoing basis on the application of international sanctions legislation and TFS guidelines, with a focus on: (I) the adoption, amendment or completion of legal acts establishing international sanctions; (II) the updating of guidelines and best practices in this area; (III) the clarification of international sanctions regimes in the financial area, in particular in relation to sanctions for frozen assets; and (iv) current and emerging risks.

The FSA has also sent direct alerts to the boards of directors of financial entities pursuant to UNSC Resolutions 2321/2016, 2371/2017, 2397/2017 regarding DPRK, UNSC Resolution 2509/2020 regarding Libya, UNSC Resolutions 2140/2014, 2216/2015, 2402/2018 regarding Ghana, UNSC 1556/2004, 1591/2005, 2340/2017 regarding Sudan, UNSC 2140/2014, 2402/2018 regarding Yemen, UNSC Resolution 2462/2019 regarding terrorism.

The assessment of the competence and good repute of the persons appointed to the board of directors of financial entities or new entrants is also carried out in the light of the international sanctions' regime. This assessment shall also cover the persons designated within the entity to coordinate the activities of the international sanctions regime (ISDP). Their assessment and notification were carried out until 02.01.2021 based on the provisions of FSA Regulation No 1/2019 (and prior to FSA Regulation No 14/2015) and from the date of entry into force of FSA Regulation No 25/2020 it is no longer necessary to notify the FSA of the documents on the basis of which the assessment is carried out, which are submitted only upon request. At the same time, the new legal framework has clarified the TFS obligations for financial entities and established dissuasive sanctions for non-compliance. The obligations set out in FSA Regulation 25/2020 relate to customer due diligence, internal control, reporting and the possibilities to request third party or humanitarian law waivers. All entities must have an internal policy for the implementation of the international sanctions regime, including elements of internal control covering all lines of business.

On-site monitoring themes include verification of compliance with the international sanctions regime and, to date, no elements of violations have been identified, but have been set out in action plans to supplement or amend aspects of internal policies, procedures and mechanisms for implementing international sanctions (2 intermediaries, 1 AIFM in 2017; 3 intermediaries in 2018; 2 intermediaries, 1 AIFM in 2019; 3 AIFM in 2020).

Sectoral vulnerabilities for non-bank financial entities in the field of international sanctions emerge from the elements identified for improvement:

- Outdated list of designated persons used for customer due diligence purposes;
- Obsolete internal procedure for TFS;
- Internal control without covering all TFS obligations;

[164] https://FSAromania.ro/ro/c/141/sanc%C8%9Biuni-internal%C8%9Bionale

- Lack of internal training for all employees carried out by the person responsible for TFS (PDSI).

These vulnerabilities result in threats that span the TFS Sectoral Assessment:
- a poor understanding of the TFS requirement and its purpose;
- Use of straw men or shills in casual transactions or business relationships through direct or indirect control of designated persons/evasion of TFS;
- Using a long/non-transparent chain of holdings to cover indirect control of designated persons for the purpose of evading TFS;
- Using financial sectors to transport money to people close to designated persons.

Risk remediation measures are also taken for TFS vulnerabilities, such as training, public list of designated persons, public warnings and direct communication with board members of supervised financial entities.
From the perspective of the implementation of the international sanctions' regimes for non-bank financial entities we assess a low degree of risk, both in terms of financial flows and products offered by non-bank financial entities and from a sectoral and national perspective.

6.3.6. Implementation of (specific) international sanctions at the level of the sector supervised by the NBR

Regarding the implementation of international sanctions in Romania, a field that also includes the regimes of sanctions related to terrorism and the financing of terrorism and the financing of acts of terrorism, as well as the regimes regarding non-proliferation, the NBR is the supervisory authority regarding the implementation of international sanctions to block funds, for financial and credit institutions that fall within its scope of activity, according to the regulations in force in the field of preventing and combating ML/TF. In this area, the authority that must carry out the necessary investigations regarding the reporting of funds or economic resources that are subject to international sanctions is NAFA.

Specifically, in the field of the implementation of international sanctions, the NBR has the following attributions regarding the financial-banking sector under its supervision:
- to oversee the application of international sanctions;
- to ensure the dissemination of acts that establish mandatory international sanctions in Romania;
- to adopt specific regulations regarding the supervision of the implementation of international sanctions;
- order specific measures or sanctions for violating the relevant legislation (Government Emergency Ordinance no. 202/2008; NBR Regulation no. 28/2009; NBR Regulation no. 7/2011; NBR Order no. 340/2010; Law no. 129 /2019; NBR Regulation no. 2/2019);
- to participate, through designated representatives, in the meetings of the inter-institutional Council established under the provisions of art. 13 of the Government Emergency Ordinance no. 202/2008 on the implementation of international sanctions.

The sector supervised by the NBR has a solid compliance culture and experience in the field, having implemented processes to identify, assess, monitor, manage and mitigate risks related to TFS.

In the context of assessing the risks arising from the way in which international sanctions are implemented by each supervised entity, the following factors are assessed, without the enumeration being exhaustive:

- analysis of the reports sent to NAFA and NBR, according to the reporting mechanism and model, regarding the designated persons and/or entities identified as a result of the application of KYC measures;
- analysis of the procedures established for updating the lists of designated persons/entities;
- analysis of authorizations, exemptions, transfer notifications regarding certain relationships that are subject to international sanctions, if applicable;
- assessment of compliance with the provisions of NBR Regulation no. 28/2009, respectively if the supervised institution has developed and submitted to the central bank the procedures for the implementation of the international sanctions of blocking funds, which include at least:

- procedures for detecting designated persons/entities;
- the regime of clients previously identified as designated persons or entities, starting from the date from which they are no longer subject to international funds blocking sanctions;
- ways of drawing up and keeping records regarding designated persons or entities;
- the access of persons with attributions in the field to the records of the institution to examine the operations carried out in the past with/by designated persons or entities;
- the competences of persons with responsibilities in the application of the relevant legislation in the field;
- the internal reporting procedures regarding the identification of a designated person/entity;
- analysis of how IT alerts are managed.

The level of risk is determined by combining two determining factors, namely the rating for inherent risk factors and the rating for factors mitigating the inherent risk resulting from the non-implementation of international sanctions, and taking into account the following factors: The likelihood of the risk materializing in transactions/operations involving the misuse of the banking/financial sector to channel illegal funds, or even funds of legal origin, for the purpose of terrorist financing; the estimated impact on the integrity, soundness, reputation and, by implication, the stability of the banking/financial system; the existence of policies, controls and procedures in place to adequately manage the terrorist financing risks identified at EU, national and supervised entity level. These policies, controls and procedures should be proportionate to the nature and size of the entities concerned.

Targeted Financial Sanctions (TFS), the listing of organizations and individuals under an international counter-terrorism sanctions regime is one of the preventive measures against terrorist activities (and also those related to the financing of nuclear proliferation).

Supervised institutions are kept informed on an ongoing basis about the application of international sanctions legislation and TFS guidelines/guidelines, with a focus on: (i) the adoption, amendment or completion of legal acts establishing international sanctions; (ii) the updating of guidelines and best practices in this area; (iii) clarifications on international banking and financial sanctions regimes; and (iv) current and emerging risks.

Also, even though the unilateral sanctions regime imposed by the US is not binding on Romanian entities, the NBR recognizes that financial institutions must comply with the OFAC (Office of Foreign Assets Control of the US Department of the Treasury) sanctions regime when their clients conduct transactions involving US correspondent banks, and the

NBR has sent information letters to the supervised system on recent developments in the OFAC sanctions regime.

As regards other types of information letters sent to the sector, the following are examples: (i) the recommendations of the UN Security Council Sanctions Committee (UNSC) 1267 (1999) on ISIL/Daesh, Al-Qaida and associated individuals, groups, undertakings and entities, which called on UN Member States to strengthen the implementation of targeted restrictive measures, of the UNSC Committee on Somalia and of the Committee established pursuant to UNSC Resolution 1718 (2006) on the Democratic People's Republic of Korea, which were included in the document entitled "Guidelines on exemptions from the provision of humanitarian assistance to the Democratic People's Republic of Korea"; (ii) Guidance on principles for managing the risk posed by the delivery of humanitarian funds to Syria; (iii) the creation of two online tools at EU level to assist economic operators to conduct business with persons/entities in Iran in compliance with international sanctions regimes, namely the "Due Diligence Helpdesk on EU Sanctions for EU SMEs Dealing with Iran" and the "EU Sanctions Tool", in order to provide useful elements for the assessment of the risks associated with conducting business activities related to Iran, which can also be used in the context of fulfilling the obligations of credit institutions, in view of the provisions of Art. 18 of Government Emergency Ordinance No 202/2008 on the implementation of international sanctions; (iv) the Guide to International Sanctions, which is a study recently issued by the Global Investigation Review, containing conceptual issues, analyses of current challenges in the field, as well as relevant elements of the UN, EU, OFAC and UK-specific post-Brexit restrictive measures regimes; (v) the results of the Chatham House/The Royal United Services Institute (RUSI) survey of several financial institutions around the world on counter-proliferation finance and the implementation of international sanctions, entitled Proliferation Finance Survey; (vi) Money Laundering and Terrorist Financing (ML/TF) risk assessments as set out in the Financial Action Task Force (FATF) public statements on identified vulnerabilities with a view to taking appropriate action, such as "Jurisdiction Subject to a FATF Call on its Members and Other Jurisdictions to Apply Counter-Measures to Protect the International Financial System from the Ongoing and Substantial Money Laundering and Financing of Terrorism (ML/TF) Risks"; (vii) third countries with a high risk of money laundering and having strategic money laundering deficiencies in accordance with Commission Delegated Regulation (EU) 2016/1675 of July 14th, 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high risk third countries with strategic deficiencies, as amended; (viii) the development by the Wolfsberg Group of the "Sanctions Screening Guidance" relevant to international sanctions; (ix) the report of the UN Security Council Sanctions Committee established pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) on ISIL (DA'ESH), AL-QAIDA and associated individuals, groups, companies and entities, etc.

Other guidelines issued by relevant international fora and presented to the supervised sector refer to: International Best Practices: Targeted Financial Sanctions Related to Terrorism and Terrorist Financing (FATF - FATF Recommendation 6)[165]; Financing of the terrorist organization Islamic State in Iraq and the Levant (ISIL)[166]; Guidance on assessing and mitigating proliferation financing risks[167]it; FATF Guidance on Combating Proliferation

[165] http://www.fatf-gafi.org/publications/fatfrecommendations/documents/bpp-finsanctions-tf-r6.html
[166] https://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organization-ISIL.pdf
[167] https://www.fatf-gafi.org/publications/financingofproliferation/documents/proliferation-financing-risk-assessmentmitigation.html

Financing - Implementing the Financial Provisions of United Nations Security Council Resolutions to Combat the Proliferation of Weapons of Mass Destruction[168]and so on.

In addition to ensuring continuous direct communication with the supervised sector, the NBR publishes updated information in this field on its official website in a dedicated section.

Another important aspect, with a significant contribution to mitigating the risk of misapplication of international sanctions, relates to the NBR's concern about the awareness of supervised institutions of the need to clarify any tendency/attempt to circumvent international sanctions and to ensure effective screening programs targeting those persons and entities associated with international sanctions, without which financial activity would be inconceivable.

In addition to the enforcement of the relevant international sanctions' legislation, a constant concern has been the awareness of supervised entities of the importance of proper enforcement of international sanctions, including from the perspective of the financial impact of compliance, reputational and operational risks. It is worth mentioning, in this context, the organization, within the framework of the national awareness program "PROTECTOR - Safe Business", of the conference dedicated to financial-banking institutions operating on the Romanian territory, which had as its objectives the real problems identified in the banking system. The main objective of the program is to warn the business environment about the risks arising from non-compliance with international sanctions aimed at making funds or economic resources indirectly available to designated persons and entities.

At the same time, with regard to the supervision of the implementation of international sanctions by entities, representatives of the NBR actively attended the meetings of the Interinstitutional Council set up to ensure the general framework for cooperation in the field of implementation of international sanctions. Specifically, the NBR has provided the documentation and expertise in the financial-banking field, necessary for: (i) the preparation of Romania's mandates and position papers, presented to international bodies with responsibilities in the field of international sanctions, in particular to the meetings of the RELEX working group - "Sanctions" formation of the Council of the European Union; (ii) the preparation and issuance of advisory opinions to support decisions on the application of international sanctions specific to its field of activity; (iii) informing the Ministry of Foreign Affairs on the measures adopted by the entities supervised by the NBR for the implementation of international sanctions established by UN Security Council Resolutions, for the purpose of drafting the Country Report, which is subsequently submitted to the UNSC; (iv) drafting the Annual Report on the measures adopted by Romania for the implementation of the sanctions regimes established at international level in the financial-banking field (for the purpose of its presentation by the Prime Minister to the Parliament and the Supreme Council of National Defence); (v) development of impact studies and analyses on the implementation of international sanctions with a view to their clarification and uniform application, e.g. in the light of FATF/FAFT Statements on vulnerabilities and risk factors in relation to nuclear proliferation and terrorist financing, etc.

[168] http://www.fatf-gafi.org/publications/financingofproliferation/documents/guidance-counter-proliferationfineancing.html,http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-UNSCRS-prolific-WMD.pdf

6.4. The nature of the threat

At present, there are no indications of terrorist financing in Romania, with the exception of one case, represented by a Romanian citizen who transferred the sum of EUR 110 to a member of the DAESH terrorist organization in order to facilitate his travel to Syria to join the Daesh terrorist organization.

By Decision no. 149/24.03.2019, the High Court of Cassation and Justice ordered the conviction of the Romanian citizen for involvement in:

- terrorist propaganda, provided for in article 33^2 paragraph (4) of Law no. 535/2004 on the prevention and combating of terrorism (in the form in force until 13.04.2019, when it was amended by Law no. 58/2019) and
- the financing of terrorism, provided for in Article 36 paragraph (1) of Law no. 535/2004 on the prevention and combating of terrorism (in the form in force until 13.04.2019, when it was amended by Law no. 58/2019).

The types of criminal offenses provided for by Law no. 535/2004

- terrorist propaganda;
- repeated access to terrorist propaganda materials as part of a radicalization process;
- receiving or obtaining instructions through self-documentation regarding the manufacture or use of explosives, firearms or any other weapons, or to commit or assist in the commission of a terrorist act.

6.5.Counter-terrorism architecture and inter-institutional cooperation; measures to prevent and counter the materialization of the threat*;*

6.5.1. At national level, the activity concerning the prevention and control of terrorism is organized and carried out in a unified manner, according to Law no. 535/2004.

To this end, cooperation in this field is carried out as the National System for Preventing and Combating Terrorism, hereinafter referred to as the SNPCT, in which the public authorities and institutions referred to in Article 6(2) of Law No 535/2004 participate.

Within the framework of the inter-institutional cooperation mechanism in the SNPCT format, the Supreme Council of National Defence acts as strategic coordinator.

For the purpose of preventing and combating acts of terrorism, the public authorities and institutions that make up the NTPCS shall carry out specific activities, individually or in cooperation, in accordance with their legal powers and competences and with the provisions of the General Protocol on the Organisation and Functioning of the National System for Preventing and Combating Terrorism, approved by the Supreme Council of National Defence.
Within the structure of the Romanian Intelligence Service - as the national authority in this field - the Counter-Terrorism Operational Coordination Centre, hereinafter referred to as CCOA, is established, through which the Romanian Intelligence Service ensures the technical coordination of the NTPCT.

CCOA has the following attributions:

a) *coordinates the activities carried out within the SNPCT, through representatives designated by the authorities and public institutions from the composition of the SNPCT;*
b) *ensures the operative exchange of data and information between the authorities and public institutions that are part of the SNPCT regarding activities of a terrorist nature;*
c) *integrates the data and information obtained, in order to establish and undertake the necessary measures;*
d) *monitors terrorist activities and promptly informs the competent authorities and public institutions within the SNPCT;*
e) *in terrorist crisis situations, it provides logistical and operational support for the operational functioning of the National Center for Anti-Terrorist Action;*
f) *transmits to the competent public authorities and institutions within the SNPCT the data and information that are the object of the undertaking of measures, according to the legal attributions.*

6.5.2. The national legislation in this area has created the necessary legislative framework for inter-institutional consultation to ensure proper information exchange and integrated risk analysis in the area of competence, ensuring effective control of terrorist risks at national level.

6.5.2.1. Reporting entities are obliged to report suspicious transactions to the NOPCML if they know, suspect or have reasonable grounds to suspect terrorist financing activities. An essential element in documenting terrorist financing activity is the ability of reporting entities to identify a terrorist financing transaction. In this context, there is a need to continue and expand awareness programs for reporting entities on the specific risks of terrorist financing.

NOPCML analyses and processes the information and, if there are indications of terrorist financing, immediately informs the Prosecutor's Office of the High Court of Cassation and Justice.

It shall also immediately inform the Romanian Intelligence Service of suspicions of terrorist financing.

The Romanian Intelligence Service (RIS) takes steps to verify and deepen the information received, according to the legal attributions, using specific means and methods. If the data reveal the preparation or commission of a crime that falls under the category of terrorist acts, including terrorist financing, all data and information held will be transmitted to the competent prosecution authorities - DIICOT being the prosecutorial structure that is competent to conduct criminal investigations in the case of terrorist offences.

6.5.2.2. If the data or information obtained do not meet the constituent elements of a crime, but show the existence of a threat to national security, national legislation allows the adoption of administrative measures aimed at preventing the materialization of the identified threat, such as: declaration as undesirable for Romania; prohibition of entry into our country; denial/cancellation of a form of international protection; denial or withdrawal of Romanian citizenship; denial or revocation of the Romanian visa.

The implementation of preventive measures is determined by the existence of a real and immediate threat, and the appropriate preventive measure is chosen taking into account the seriousness of the actions and the imminence of the threat. The application of preventive

measures offers the advantage of immediate effectiveness and countering the materialization of the threat.

On the basis of specific assessments of persons who represented terrorist risk factors, both for Romania and for other Western European countries, to which most of them intended to travel, the Romanian authorities adopted preventive measures whereby their movement was blocked or persons were removed from Romania to their country of origin or to a safe third country when their life was not safe in their country of origin.

Every year, the authorities have identified foreign nationals from states with terrorist concerns, who either arrived in Romania or tried to enter the national territory and who had a history of fighting or who were/were affiliated with terrorist organizations such as: Daesh, Al Qaeda, Hamas, Palestinian Islamic Jihad (PIJ) etc.

Preventive measures also include removing or blocking access to terrorist content online. To this end, the National Authority for Administration and Regulation in Communications (ANCOM) has been empowered to issue a decision to block access by Romanian users to terrorist propaganda material hosted on servers located abroad and to issue orders to remove terrorist online content hosted on Romanian servers.

Conclusion

So far, no networks have been identified on the national territory operating for the purpose of obtaining, collecting or transferring funds for the benefit of terrorist organizations/entities/groups.

The international climate regarding terrorism, persons/entities issuing/distributing and/or trading any form of electronic money/virtual assets, money remittances through money transfer service providers with an extensive network of global agents, including hawala and other informal money and value transfer systems, are considered/approached by the authorities as elements of risk in relation to TF, even if they have not manifested themselves in Romania.

Since the prevention of terrorist financing activities remains a priority at institutional level and within the framework of the NTPFTS, the authorities with powers in the field of reference have permanently adopted a preventive-anticipatory approach in the management of suspicious situations, constantly monitoring and assessing the level of risk generated by persons suspected of engaging in/carrying out terrorist financing activities.

In the area of preventing and combating terrorism (including financing activities), inter-institutional and international information exchange is constantly considered. The mechanisms already in place allow for an appropriate level of cooperation, and it is appropriate to facilitate rapid and secure cross-border access to financial data for early detection of operations.

Therefore, the risk of terrorist financing in Romania can be assessed as Low

Acronyms

EBA	European Banking Authority
ANCOM	National Authority for Administration and Regulation in Communications
ANEVAR	National Association of Authorized Appraisers from Romania
AML	anti money laundering
BO	Real beneficiary
— CCJ	Other Courts of Cassation and Justice
CAFR	Chamber of Financial Auditors from Romania
CECCAR	Chamber of Certified Accountants and Certified Accountants from Romania
CTC	Chamber of tax consultants
CDD	Customer due diligence
AML/CTF	anti money laundering/control of terrorist financing
CTR	Cash Transaction Report
DIOCT	Directorate for the Investigation of Organized Crime and Terrorism
HRTC	High-risk third countries
RTE	Foreign Transactions Report
DNFBP SITES	Designated non-financial activities and professions
FG	Focus group
FSA	Financial Supervisory Authority
FZ	Free trade zone
GDP	Gross domestic product
POHCCJ	The Prosecutor's Office attached to the High Court of Cassation and Justice
IPR	Intellectual property right
TH	Law enforcement authority
ML/TF	Money Laundering/Terrorist Financing
MF	The Ministry of Finance
MJ	Ministry of Justice
ANAB	The National Agency for the Administration of Undisposed Assets
NAFA	National Agency for Fiscal Administration
EMII	Electronic money issuing institution
IF	Financial institution
NBFI	Non-banking financial institution
NBR	The National Bank of Romania
NIA	National Integrity Agency
NOPCML	National Office for the Prevention and Control of Money Laundering
NGO	Non-profit organization
ONRC	National Trade Register Office
OCG	Organized criminal groups
ONJN	National Gambling Authority
PEP	Publicly exposed person
PI	Payment institution
PFA	Authorized person
TO	Corporation
SCA	Limited company on shares
SCS	Simple limited company

SNA	National anti-corruption strategy
CNS	Company in collective name
SRL	Limited liability company
SRB	Self-regulatory body
STR	Suspicious Transaction Report
TCSP	Service providers for companies or trusts
UNPIR	The National Union of Insolvency Practitioners from Romania
UNNPR	The National Union of Public Notaries
FIU/FIU	Financial Information Unit
NAD	National Anti-corruption Directorate