Republic of Serbia
MINISTRY OF FINANCE
Administration for the Prevention of Money Laundering

Number: ON-000431-0001/2025
Belgrade, 9. 5. 2025 .

Based on Article 6, paragraph 1 of the Law on the Prevention of Money Laundering and Financing of Terrorism ("Official Gazette of the Republic of Serbia", No. 113/17, 91/19, 153/20, 92/23, 94/24) and 19/25 hereinafter referred to as: the Law), Article 38, paragraph 1 of the Law and Article 114 of the Law, and in connection with Article 105, paragraph 1 of the Law, the Director of the Administration for the Prevention of Money Laundering hereby issues

GUIDELINES FOR ASSESSING THE RISK OF MONEY LAUNDERING, TERRORISM FINANCING AND WMD PROLIFERATION FINANCING, FOR ENTREPRENEURS AND LEGAL PERSONS ENGAGED IN PROVIDING ACCOUNTING SERVICES AND FOR FACTORING COMPANIES

These Guidelines regulate the manner in which an obliged entity supervised by the Administration for the Prevention of Money Laundering prepares an analysis of the risk of money laundering, terrorist financing and proliferation of weapons of mass destruction , the procedure for determining whether a client or the beneficial owner of a client is an official, the procedure for determining whether a client or a legal person appearing in the ownership structure of a client is an offshore legal person, as well as the manner of applying other provisions of the regulations governing the prevention of money laundering and terrorist financing.

An obliged entity supervised by the Administration for the Prevention of Money Laundering is considered a legal person, i.e. an entrepreneur engaged in the provision of accounting services and a factoring company.

The Guidelines aim to raise obliged entities' awareness of their role and place in the system for preventing money laundering and terrorist financing, as well as to emphasize the importance of implementing all legal and regulatory regulations in this area, as this is the only way to effectively combat money laundering and terrorist financing.

The general part of these Guidelines is applied by entrepreneurs and legal entities engaged in the provision of accounting services and factoring companies, while the special part of these Guidelines is applied by the obliged entity to whom that part applies, taking into account the specific circumstances related to the risks that apply only to that obliged entity.

GENERAL SECTION

Money laundering and terrorist financing – a *concept*

Money laundering and terrorist financing are global issues that can negatively affect the economic, political, security and social structure of a country. The consequences of money laundering and terrorist financing undermine the stability, transparency and efficiency of a country's financial system, cause economic disruption and instability, and damage the country's reputation and threaten national security. Risks from money laundering and terrorist financing also arise from failures in the application of regulations, where the obliged entity may be significantly exposed to the risk of damaging his own reputation and reputation in the event of a fine imposed by a supervisory authority.

In the case of money laundering, the original assets always come from illegal activities, while in the case of terrorist financing the sources can be both legal and illegal. However, the main objective of those involved in terrorist financing is not necessarily to conceal the source of the funds, but to conceal the nature of the financed activity. When individuals seek to invest money from legal activities in financing terrorist activities, the funds are more difficult to detect and trace, since the transactions are in smaller amounts.

An effective system for combating money laundering and terrorist financing includes a money laundering risk analysis, a terrorist financing risk analysis, and a proliferation risk analysis .

Money laundering - definition and stages

Money laundering is the process of concealing the illegal origin of money or assets acquired through crime.

Money laundering, within the meaning of the Law, is considered to be: the conversion or transfer of property acquired through the commission of a criminal offense; concealment or misrepresentation of the true nature, origin, location, movement, disposition, ownership or rights relating to property acquired through the commission of a criminal offense; acquisition, holding or use of property acquired through the commission of a criminal offense. Money laundering, within the meaning of the Law, also includes the above-mentioned activities carried out outside the territory of the Republic of Serbia.

When the proceeds of crime are obtained, the perpetrator seeks a way to use the money without attracting the attention of the authorities. He therefore carries out a series of transactions that serve to present the money as legally acquired. Money laundering has three basic stages:

1. **The first phase**: the " placement" phase is the breaking of the direct link between the money and the illegal activity through which it was acquired. In it, the illegally acquired money is

introduced into the financial system. The money is deposited into bank accounts, most often in the form of some legal activity in which payment is made in cash. One way is to establish a fictitious company that has no business activities, but serves exclusively for depositing "dirty" money or structuring large sums of money, and then depositing it into accounts in amounts that are not suspicious and are not subject to reporting to the competent authorities.

2. **Second phase**: the " ayering" or " disguise" phase. After the money has entered the legal financial system, it is transferred from the account in which it was deposited to other accounts of companies with the aim of presenting some fictitious business activity or to carry out some legal business (trade or service) with companies that operate legally. The main goal of these transactions is to conceal the connection between the money and the criminal activity from which it originates.
3. **The third phase**: the "integration" phase, in which "dirty" money appears as money originating from legal activities. A common method of integrating "dirty" money into legal financial flows is the purchase of real estate or the purchase of controlling stakes in joint-stock companies, which is an example of the concentration of "dirty" capital on a large scale, which is the goal of the "money launderer". Integration focuses on market values, i.e. on what can be bought and sold. Leasing real estate is legal, and the income from the rent is not suspicious. Money is often invested in companies with business difficulties, which then continue to operate successfully, and the results of operations represent legal income. Once money reaches this phase, it is very difficult to detect its illegal origin.

The illegal acquisition of property is the main, if not the only, motive for organized crime. In order to enjoy the benefits of crime, the property must be falsely presented as legal.

The placement of dirty money in Serbia is significantly influenced by the country's position in the Balkan route, through whose territory illegal goods and funds transit distributed by organized criminal groups. Proceeds from criminal activities in other jurisdictions, especially from smuggling and drug trafficking, aggravated theft and fraud enter the Serbian financial system through cross-border cash transactions, transfers and other cash transactions.

According to the findings of the latest money laundering risk assessment, the layering phase of dirty money in Serbia is characterized by the use of simulated business activities and shell companies. In this way, there is an illusion of regular business transactions, with an aim to conceal the illegal origin of funds. Criminal networks establish companies and establish a structure of interconnected entities, such as shell companies in agriculture or in trade in secondary raw materials that facilitate multiple transfers using false invoices and documentation. These transfers are usually in round amounts and enable the separation of funds from their illicit source. After that, through individuals, *money laundering* companies or businesses, intended for further layering, funds are transferred to the final recipients. To this end, the services of certain professionals which are obliged entities according to the Law, such as accountants, are also used.

When it comes to the integration phase, in the period 2021-2023, the real estate and high-value goods markets in Serbia were particularly susceptible to integration, as illicit funds are

reinvested in real estate, luxury vehicles and other valuable assets. Associated and close front persons are often used to register the assets.

Money laundering profile in Serbia

The overall profile of money laundering in Serbia in the period 2021 to 2023 is dominated by the placement of criminal proceeds originating from predicate crimes committed in Serbia. There are also cross-border money laundering cases with regional and European cross-border elements. When it comes to exposure to large and complex money laundering schemes, they are not common in Serbia primarily due to the economy's focus on domestic market and financial system that does not have developed, complex, innovative or efficient financial services. Serbia is characterized by simpler money laundering models. The current trend of economic growth in Serbia is accompanied by a corresponding increase in the risk of integration of illegal funds.

Risk assessment

Risk assessment is carried out:

- at the state level (national risk assessment);
- at the sector level (sectoral risk assessment);
- at the obliged entity level;
- at the level of the business relationship (a client).

In accordance with Article 6 of the Law, obliged entities are obliged to take into account the risk assessment at the state level (national risk assessment) when preparing a risk analysis at the obliged entity level, i.e. a risk analysis in relation to their entire business (so-called self-risk assessment), as well as when preparing a risk analysis at the business relationship (a client) level.

When preparing a risk analysis at the obliged entity level, i.e. in relation to its entire business, the obliged entity is obliged to take into account the level of threat and sectoral vulnerability of the sector to which the obliged entity belongs according to the results of the national risk assessment, and, in the event that the client is also an obliged entity subject to the Law, when preparing a risk analysis at the level of the business relationship (a client), the obliged entity shall take into account the level of threat and the sectoral vulnerability of the sector to which the client belongs. In particular, when preparing a risk analysis at the level of the obliged entity, obliged entity shall take into account the level of risk of the legal form assessed by the national risk assessment , and to which the obliged entity belongs, and when analyzing the risk at the level of the business relationship (a client), the obliged entity shall take into account the level of risk of the legal form, as assessed by the national risk assessment , to which the client belongs, regardless of whether the client is an obliged entity.

In addition to the above, pursuant to Article 6 of the Law, the risk analysis must be prepared in accordance with both the Law and the Guidelines of the supervisory authority.

If a client is high-risk under the Law itself (e.g. if the client or the beneficial owner of the client is an official or if the legal person is an offshore entity or there is an offshore entity in its ownership structure or the client is not physically present when establishing a business relationship), the obliged entity shall classify such a client as high - risk for money laundering and terrorist financing and shall apply enhanced CDD measures in relation to it. Therefore, when preparing a risk analysis, such a client must be classified as high - risk under the Law itself .

Also, when preparing a risk analysis, the obliged entity is obliged to perform the risk analysis in accordance with the Guidelines of the supervisory authority, i.e., during the self-assessment of risk, it is obliged to take into account the criteria for risk analysis at the obliged entity level that are defined in these Guidelines, and when analyzing risk at the level of a business relationship (client), the obliged entity is obliged to take into account the criteria for risk analysis at the level of a business relationship (client) , i.e., to assess geographical risk, client risk, service risk, and factoring companies are obliged to assess a transaction risk as well,, the criteria for which are defined in a separate part of these Guidelines .

Serbia applies a comprehensive approach to identifying, assessing and understanding its risks. The central element of the system is the periodic activity of the National Risk Assessment (NRA), which is mandatory by law to be carried out every 3 years, starting in 2018. The competent authorities of the Republic of Serbia have consistently met these legal deadlines, and have thus carried out the following NRAs:

- 2018: money laundering, terrorist financing, risk assessment for NPOs, as well as legal persons and legal arrangements;
- 2021: money laundering, terrorist financing and proliferation financing, as well as additional modules for risk assessment of legal persons, non-profit organizations, VASPs
- 2024: money laundering, terrorist financing and proliferation financing, as well as additional modules for risk assessment of legal persons, legal arrangements (i.e. persons under foreign law) , non-profit organizations, VASPs.

The World Bank methodology was used to assess the risk of money laundering and terrorist financing, and the same methodology was also used to assess the risk of commercial entities and legal arrangements and to assess the risk of misuse of the NPO sector for the purpose of terrorist financing.

The Council of Europe methodology was used to assess the risk of money laundering and terrorist financing in the digital asset sector, while the methodology developed by Serbia using the FATF methodology and the FATF Guidelines on Proliferation, as well as experience from the previous risk assessment using the RUSI methodology, was used to assess the risk of proliferation of weapons of mass destruction.

During the work, certain criteria from the methodologies were supplemented in a way that took into account the specificity of the state - the legal institutions that have been established, the geopolitical location, the geographical position of Serbia, the position of Serbia in the international environment, and certain criteria from the methodology, as stated, underwent appropriate adjustments in order to assess the risk as objectively as possible.

In this way, the unique economic, geopolitical and cultural context of the country was respected.

Also, the Expert Team of the Coordination Body for Cross-Border Threats Review, formed in 2019, supplemented the criteria from the World Bank methodology relating to cross-border threats, taking into account the geographical position of the country, international cooperation, client structure and risk by residency of the obliged entity and data exchange.

This innovative list of criteria was used both for the assessment of cross-border threats and in the assessment of risk in 2021, with the World Bank methodology, as well as in the current risk assessment.

In addition to the above, representatives of the Risk Assessment Working Group (the National Coordinator and WG Heads) during the implementation of the 2018 risk assessment developed their own criteria for assessing the risky forms of business entities, taking into account the legal and institutional framework and the process of registration and operation of business entities in Serbia, so that the risks characteristic of the country could be detected and objectively assessed. In this risk assessment these criteria were also used for the final risk assessment.

The concept of risk, risk assessment, threat , vulnerability and consequences

- ***Risk*** is a function of three factors: threat, vulnerability, and consequences.
- ***Risk assessment*** is a product or process that is achieved, or rather, carried out based on a methodology that seeks to identify, analyze and understand the risks of money laundering and terrorist financing and represents the first step towards their mitigation. Ideally, a risk assessment contains assessments of threats, vulnerabilities (weaknesses) and consequences.
- ***A threat*** is a person or group of persons, an object or an activity that has the potential to cause harm, for example, to a state, society, economy, etc. In the context of money laundering and terrorist financing, this includes persons engaged in criminal activity, terrorist groups and their enablers, funds and assets in the broadest form at their disposal, as well as past, current and future money laundering and terrorist financing activities.
- ***The term vulnerability*** or weakness used in risk assessment refers to parts of a system through which a threat can be realized or which can contribute to or enable the performance of activities implied by a threat, i.e. a series of mechanisms that can be a deterrent to the realization of a threat.
- ***Consequence*** refers to the impact or damage that money laundering or terrorist financing can cause and includes the effect that the predicate crime and terrorist activity can have on financial systems and institutions, as well as on the economy and society in general. The consequences of money laundering or terrorist financing can be short-term or long-term and reflect on the population, specific communities, the business environment, national or international interests, as well as the reputation and attractiveness of the financial sector in the country.

When talking about risk assessment, it is necessary to keep in mind that the assessment includes inherent risk and residual risk. Inherent risk implies the result of threats and vulnerabilities that are specific to a particular sector. This level of risk is influenced by various factors, primarily the quality and effectiveness of prevention and repression measures applied by the competent authorities. These factors can reduce the level of risk, if there is consistent and effective law enforcement, well-developed supervision, adequate capacity, etc., which ultimately results in a lower residual risk. A lower residual risk, viewed from the perspective of, for example, the obliged entity, can be influenced by a number of control mechanisms that contribute to reducing the risk of a particular product, service, business practice or method of providing a particular product or service.

The findings of the latest money laundering risk assessment is that the dominant methods of money laundering in Serbia are:

- Simulated business activities: Money laundering through non-existent or inflated business activities and the siphoning off of funds through associated persons, often involving entrepreneurs, agricultural holdings, and service providers.
- Interconnected business transfers: A network of entities linked by ownership structure, which transfers funds based on false business documentation in order to conceal the illegal origin of the funds.
- Transfers to individual accounts: Funds are ultimately transferred from corporate accounts to individual accounts, often based on the purchase of secondary raw materials or agricultural products.
- Shell companies: Companies established and intended solely for the purpose of laundering funds without any real economic activity, often called laundering or phantom companies.
- Use of businesses: Individuals open businesses, especially with the aim to facilitate the withdrawal of cash involved in money laundering.

Money laundering threat assessment

The ML threat assessment focuses on predicate crimes, the involvement of organized crime, various forms of seizure/confiscation of assets and property, criminal proceeds and the economic losses to the state as a result. High-threat crimes determined on this basis are: tax crimes, fraud in commercial operation, drug trafficking, corruption in the public sector, fraud and organized crime.

The value of assets that pose a threat to money laundering is estimated at almost 1.5 billion Euros and consists of discovered property gains from filed reports, dark figures, confiscated assets, as well as assets that were the subject of money laundering in letters rogatory sent to Serbia.

Assets posing a money laundering threat in Serbia worth EUR 1,563,275,393 represent 0.80% of Serbia's GDP

In relation to the declared level of threat, the share of confiscated assets in criminal proceedings of EUR 165,179,934 represents 10.5% of the total money laundering threat.

The largest amount of confiscated property is recorded in criminal offences committed by organized criminal groups.

This concerns assets worth a total of EUR 21,011,238, which were confiscated on various grounds, which is 12.72% of the total confiscated assets or 23.50% of the total money laundering threat from organized crime.

In the investigations initiated, the abuse of position of a responsible person as a predicate offense recorded the largest amounts of property involved in money laundering, EUR 22,507,963. This constitutes 13.50% of the estimated property gain for this offense. The situation is similar with the investigations of tax offenses, from which the value of property involved in money laundering is EUR 23,573,192, which is 6.53% of their total estimated property benefit.

Factors that influence the increased level of threat:

Insufficient number of money laundering proceedings initiated for certain criminal offences: Although the values of assets that have been discovered and seized, as well as their estimated values, are in line with global trends, and in certain predicate criminal offences, a significant volume of the estimated proceeds is covered by criminal proceedings for money laundering; it is necessary to increase the number of money laundering cases for certain criminal offences, both in terms of the number of persons prosecuted and in terms of the assets covered by money laundering. This applies primarily to corruption criminal offences, where the current situation is explained by the fact that the amounts of illegal proceeds in these cases are low and did not require the participation of third clients in their laundering. In addition, the focus of the competent authorities when it comes to prosecuting for money laundering is cases in which significant illegal assets have been generated. In such situations, proceedings for money laundering have also been initiated, as is clearly seen from the case study.

Even with proceeds acquired through illicit drug trafficking, the number of criminal proceedings initiated for money laundering is small, and this practice must change in the coming period, despite the fact that the amounts of property seized in the aforementioned criminal offenses are extremely high.

Factors that reduce the likelihood of money laundering threats:

Value of seized assets: The rate of seized assets is higher than the global average.

Significant amounts of discovered property that was the subject of money laundering: For certain predicate crimes such as tax crimes and abuse of position of a responsible person, significant amounts of property in money laundering cases have been detected and prosecuted. Also, for certain crimes such as drug trafficking, high amounts of property have been seized, so the threat of money laundering has been eliminated to a large extent.

The risk assessment of different sectors, as well as the list of crimes that pose a higher level of risk, have changed in the last three risk assessments, as can be seen from the following graph.

2018		2021		2024	
В	Банке	В	Некретнине	В	Некретнине
	Онлајн приређивачи игара на срећу		Онлајн приређивачи игара на срећу		Адвокати
	Некретнине		Банке		Рачуновође
СВ	Казина	СВ	Рачуновође	СВ	Банке
	Рачуновође		Мењачи		Мењачи
	Мењачнице		Казина		Јавни бележници
С	Јавни бележници	С	Посредници у промету непокретности		Посредници у промету непокретности
	Адвокати		Адвокати		Онлајн приређивачи игара на срећу
СН	Тржиште капитала	СН	Факторинг друштва		Пружаоци услуга дигиталне имовине
	Платне институције и институције електронског новца		Тржиште капитала		Казина
	Ревизори		Платне институције и институције електронског новца	С	Поштански оператори
Н	Добровољни пензијски фондови		Ревизори		Ревизори
	Друштва за осигурање		Јавни бележници		Платне институције и институције електронског новца
	Даваоци финансијског лизинга	Н	Даваоци финансијског лизинга	НС	Тржиште капитала
			Друштва за осигурање	Н	Факторинг друштва
			Добровољни пензијски фондови		Даваоци финансијског лизинга
			Поштански оператори		Друштва за осигурање
					Добровољни пензијски фондови

Display of the risk level of different sectors

high-risk offenses includes the following:

Tax crimes

- Tax crimes have the highest estimated illegal property gain, i.e. 360 million euros. Tax crimes as predicate crimes for the money laundering offense are specific because the laundering process often involves multiple sectors, with the banking sector playing a central role. This is expected, as entities that evade tax obligations usually have bank accounts where funds withheld from public revenues are deposited.
- In addition, accounting service providers play a key role in facilitating money laundering in these schemes. The final integration of laundered funds is usually achieved by depositing cash into the accounts of legal entities based on the founders' loans, increasing the founders' shares, or purchasing valuable goods for the owners' personal needs. In some cases, these funds are used to pay unrecorded salaries to employees, thereby avoiding taxes and contributions on wages.
- A significant part of money laundering from tax offenses is associated with the "grey" economy, where unregistered activities are used to avoid tax obligations. The latest analysis of the scope of the grey economy in Serbia from 2022 showed that the scope of the grey economy in the last five years among registered businessmen has decreased from 14.9 to 11.7 percent of GDP, which amounts to as much as 6.5 billion Euros. It is estimated that every fourth company is involved in the grey economy, while five years ago it was every third. According to an alternative, monetary calculation method, the findings on the grey economy also show a downward trend from

22.2 to 20.1% of GDP in the past five years. The sector most vulnerable to the grey economy is construction, where every fifth company is in the grey economy (as well as in the manufacturing industry), and as many as 13% of workers are informally employed; the agricultural sector is in the second place. In the overall legal economy, the share of employees in the black labour market has fallen from 11% to 8.5% in the past five years, and the number of informally employed workers has decreased by 200,000, which is further confirmation of the decline of the grey economy.

Corruption in the public and private sectors

Corruption is one of the biggest threats underlying the criminal offence of money laundering.

- Corruption crimes in Serbia encompass a wide range of key predicate crimes, including abuse of office, active and passive bribery, as well as crimes related to embezzlement and misappropriation, especially in the area of public procurement.
- The total damage from corruption-related crimes is significant, estimated at 33.5 million Euros. These crimes often involve the abuse of position by public officials for personal gain, with serious consequences for state institutions and public trust.

Authorities are using a multi-layered approach to address this threat:

- the first priority is to focus on detecting third-party money laundering and all actors within obliged entities who could be involved in laundering corruption-related proceeds, where such cases have been identified in practice;
- the second aim is to prosecute ML in connection with the predicate offence. Here, in the last year, Serbia has intensified its efforts to tackle corruption through a national law enforcement campaign that has led to a significant increase in investigations and prosecutions of high-profile corruption cases in both the public and private sectors. In each of these cases, money laundering is pursued in parallel as a related offence. This integrated prosecutorial practice serves as clear evidence that Serbia is seriously committed to combating the common threat of money laundering, where corruption is the underlying offence.
- third, when there is no money laundering – which implies that the income obtained through criminal acts of corruption is directly confiscated;
- Fourth – to use the resources of AML/CFT institutions such as the Anti-Corruption Agency to assist anti-corruption authorities in implementing preventive measures, including through facilitating international cooperation.

Additional points:

- “Abuse of office” and “abuse of position of a responsible person” are considered the main predicate offences related to corruption in the public and private sectors with a total estimated illegal property gain of 199 million Euros. The latter offence is also the integral part of the repressive policy in the field of AML when it comes to obliged entities involved in illegal activities, including money laundering or fraud-related operations. In such cases, the criminal

offence of "abuse of position of responsible person" would be used against the management or employees of the obliged entity in parallel with the criminal offence of ML, or separately, when ML could not be proven.

- When it comes to corruption in the public sector, complex cases have been identified in which corrupt officials hired employees of obliged entities for the purpose of money laundering.

Drug trafficking

In drug-related crimes, the proceeds were estimated at 128 million Euros. These crimes are closely linked to organized crime (see below).

Organized crime offences

- It is estimated that organized crime generates proceeds of crime in the amount of 89 million Euros, however, it should be noted here that a significant part of the estimated proceeds of crime in other categories of crimes can be transversally attributed to organized crime, which permeates these other spheres of criminal behavior, especially some more sophisticated criminal operations.
- Organized crime groups in Serbia, especially mafia-type organizations, maintain strong ties with transnational criminal networks involved in drug trafficking. These groups participate in all stages of the drug trafficking process, from the procurement of narcotics — often from Latin America — to organizing their transport to Europe and overseeing their distribution across the continent. Sophisticated methods are used to conceal drugs in commercial goods such as slabs of concrete, chemicals and bananas, while innovative technologies are used to evade customs checks and conceal their communications. Members are predominantly Serbian citizens or individuals from the wider Balkan region.
- In addition to drug trafficking, these groups are involved in a wide range of illegal activities aimed at consolidating their dominance in the criminal underground. These activities include money laundering, trade in influence, and violent crimes such as murders targeting rival groups, which often spread beyond Serbia to Europe and South America. The sale of cocaine in Serbia helps finance violent operations and maintain group cohesion. Recruitment focuses on younger individuals, especially members of violent sports fan groups or ex-convicts with a history of violent crimes.
- Despite operating primarily outside Serbia, these groups integrate illicit proceeds into the domestic economy through money laundering. This is achieved by purchasing real estate, investing in construction projects, purchasing luxury goods, and financing legitimate businesses. To counter this, Serbian prosecutors are using international cooperation mechanisms, leading to the seizure of assets in Serbia, as well as in Montenegro, Spain, and beyond.
- The growing sophistication of money laundering methods among organized crime networks required the establishment of a standing working group for combating organized and

serious crime within the Public Prosecutor's Office for Organized Crime (PPOC), established in December 2020, which successfully dismantled 11 groups in 13 criminal proceedings involving 189 individuals during the reporting period. Notable cases include the "Balkan Cartel", which smuggled over seven tons of cocaine across multiple countries, using methods such as simulated legal transactions and covert transport. Assets related to these operations, including cash, real estate and luxury items, were seized. This case highlights the extensive resources and international context of Serbian organized crime's involvement in regional and international operations, as well as the capacity of the relevant authorities to address the threat.

- The rise of digitalization and globalization is transforming the way these criminal groups operate. They now use encrypted communications, cryptocurrency-based money laundering schemes, and advanced smuggling technologies to hide their activities and evade law enforcement.

Fraud

The proceeds of the fraud were estimated at €36 million. The fraud has been recently moved to the high-risk category, the only change to this list since the 2021 NRA. This update was made to take into account the growing risks of high-tech fraud and related cross-border money laundering trends.

Criminal offenses in the medium risk category
Human smuggling and human trafficking

In previous risk assessments, these crimes were classified as high-threat, for a number of reasons, such as the peak of the "migrant crisis", the number of organized crime groups prosecuted for this crime, the creation of new criminal groups that cooperated with criminal groups from other countries, as well as the property gains that were detected and confiscated from the perpetrators of this crime. Due to the inclusion of the territory of Serbia in the migrant route, it was inevitable that individuals and groups from these areas would be involved in smuggling chains, and their role was to transfer migrants from southern Serbia to the EU border in the north This crime is usually committed by ad hoc criminal groups. The current risk assessmen shows that there has been a decrease in the number of migrants, a decrease in the number of organized crime groups and lower-level criminal structures that are engaged in this criminal activity on an international scale. This has led to a reduction in the threat level for this underlying crime.

Forgery of documents, fraud in the performance of economic activities, illicit trade and entrepreneurship

These activities constitute a key set of economic crime offences with milder consequences for society but still significant in terms of the volume of criminal proceeds that contribute to the

criminalization of economic activity in Serbia and the region. These offences are also often accompanied by money laundering activities by organized crime groups and money laundering professionals (e.g., document forgery), which requires continued attention to the money laundering component in addition to these predicate offences, and vice versa.

Illegal construction (construction without a permit)

This crime generates significant revenue, and its enforcement is a key priority in the state's efforts to reduce the grey economy and bring transparency to the real estate sector, which is a key vehicle for the layering and integration of money laundering in Serbia.

Money laundering vulnerability assessment

Regarding the vulnerability assessment, the NRA examines both national-level factors in accordance with the Methodology, as well as sectoral vulnerability factors.

- Cases of employee integrity deficiencies have been observed in a number of sectors, suggesting a material vulnerability. Given that such cases are systematically identified in foreign jurisdictions with comprehensive AML/CFT systems (e.g. UK, US, Switzerland, Germany and others), the competent authorities in Serbia have prioritized the identification of such facts through cross-examination of reporting forms and suspicious transaction report , as well as through effective cooperation between law enforcement and supervisory authorities. Additional measures have been implemented to mitigate this vulnerability, e.g. through direct licensing and periodic testing of AML/CFT compliance officers by APML. The Serbian authorities consider this vulnerability a priority, particularly due to the potential damage that a single problematic officer at an obliged entity could cause to the integrity of the AMLK/CFT system by enabling the laundering of significant amounts of funds, as demonstrated by cases in domestic and foreign jurisdictions. In terms of sectors, this vulnerability is a priority for banks, lawyers and accountants.
- Other systemic vulnerabilities include the systemic use of cash in the remittance sector, as well as the significant number and turnover of obliged entities in the currency exchange sector, which require the engagement of significant resources in supervision .
- Regarding DNFBPs, although the general awareness of risks is good (with some exceptions), vulnerabilities in some sectors are reflected in the low number of suspicious transaction reports (STRs) , and the lack of resources for effective implementation of internal controls.
- Regarding VASPs, Serbia has carried out two risk assessments, in 2021 and 2024, given that the first Law on Digital Assets entered into force in 2021. The materiality of the sector is considered low, given that only 2 VASPs are in operation, given the strict licensing regime and the effectiveness of inspection controls under the jurisdiction of the NBS; however, the development of new technologies in this sector requires constant attention and investment as a priority for the area of law enforcement and supervision, and all this resulted in a medium-high risk assessment for this sector.

Understanding sector risks

The overall risk profile in the financial institutions and VASPs sector, including threats, vulnerabilities and resulting money laundering risks, is presented in the following table:

Sector	Threat	Vulnerability	Risk
Banking sector	**High**	**Medium**	**Medium-high**
Leasing sector	**Medium**	**Low**	**Low**
Life insurance sector	**Low**	**Low**	**Low**
Voluntary Pension Fund Management Companies Sector	**Low**	**Low**	**Low**
Sector of persons providing money and value transfer services / e-money institutions	**Medium**	**Medium**	**Medium**
Exchange office sector	**High**	**Medium**	**Medium-high**
Factoring sector	**Medium**	**Low**	**Low**
Capital Markets Sector	**Low**	**Medium-low**	**Medium-low**
PUDI Sector	**High**	**Medium**	**Medium-high**

Factoring companies pose a low risk in terms of ML/TF, given the small size of the sector, the limited nature of the business, comprehensive controls and oversight, and the very high culture of compliance in the sector.

The overall risk profile of the DNFBPs sector, including threats, vulnerabilities and resulting risks, is presented in the following table:

Sector	**Threat**	**Vulnerability**	**Risk**
Casino	High	Medium	Medium-high
Games of chance via electronic means of communication - online	High	Medium - high	Medium-high
Real estate agents	Medium-high	Medium - high	Medium-high
lawyers	High	High	High
Accountants	High	Medium - high	High
notaries	Medium-high	Medium	Medium-high

Serbia considers the accounting sector to be one of the most important sectors in terms of preventing and protecting against money laundering, given that accountants usually have direct knowledge of the flows of money and its origin in companies and that in most cases they know their clients very well. Accountants are mostly misused, both knowingly (as 'professionals') and

unknowingly, in complex money laundering schemes involving legal persons and various types of economic and commercial operations for the purpose of money laundering.

They often appear in the role of persons carrying out business registration activities, and a preventive arrangement has been introduced as a measure to collect information for *gatekeepers* through the recently introduced requirements in the Law on the Central Records of Beneficial Owners . These oblige *gatekeepers* to disclose their status when incorporating and registering companies, and accountants have in a large number of cases already disclosed their role in the process.

Given their sectoral specificity, accountants are a particular subject of interest for supervisory and law enforcement authorities in terms of identifying their potential proactive participation in professional money laundering schemes . In the analyzed period, an investigation was initiated for the criminal offense of money laundering against 8 persons, and 6 persons who were certified accountants were charged, while 3 persons who performed the duties of accountants were convicted in the final proceedings. This demonstrates, on the one hand, a high - level threat environment in the sector, and on the other hand, the ability of the competent authorities to identify and partially mitigate this threat through specific enforcement results.

Analyzing the modus operandi of the crimes in which accountants were involved, it was determined that they had mainly assisted by providing advice on the method of money laundering through incorporating business entities, issuing fictitious invoices, which were used both for unjustified payments and unjustified VAT refunds, recording these invoices , preparing tax returns with unjustified VAT, withdrawing money from the business accounts of business entities based on fictitious invoices or money that was refunded based on unjustified VAT refunds and handing that money over to the payer.

The specific modalities of engagement of accountants are summarized in the 2021 and 2024 NRAs and described in more detail in all typology reports prepared by the APML. Furthermore, it should be emphasized that certain FT probabilities were identified in the previous reporting period (prior to 2019) in relation to accountants, in particular with regard to possible links to TF operations related to NPOs.

Risks of terrorist financing

A large number of terrorist threats have emerged within and around Serbia, as well as neighboring regions, including:

- self-radicalized individuals,
- ethno-separatist movements,
- ideological and religious extremism,
- regional networks,
- Foreign terrorist fighters and conflicts abroad

All of the above potentially supports terrorist financing activities through numerous channels used by terrorist financiers (payment institutions, exchange offices, financial technologies and NPOs), which can partially penetrate the Serbian financial system.

Considering the inherent threats and existing controls, the NRA considers that **terrorist financing poses a medium risk** to Serbia's objectives set out in its National Security Strategy, in

particular in ensuring its stability and security of the country and its citizens, as well as efforts to prevent terrorism in neighboring regions.

After one successful prosecution and conviction in the period 2016-2019 for terrorist financing, involving international transfers and NPOs, no new cases of terrorist financing were identified in Serbia in the period 2019-2023.

Hypothetical scenarios:

- Self-radicalized individuals, who are often active onlin , can potentially attract external funding for their activities.
- Recent terrorist acts in 2024, ethnic separatism, and ongoing regional instability, particularly in Kosovo and Metohija, could also attract financial support from sympathizers and extremist networks abroad.
- Extremists can manipulate vulnerable populations, including religious converts and economically disadvantaged individuals, into unwittingly supporting FT .
- In addition, cross-border ethnic ties and regional movements can foster the development of FT networks.
- Given the experience of previous prosecutions, NPOs continue to pose a risk for FT , along with potential abuse by *gatekeepers*, such as accountants.
- Alternative remittance systems, as well as formal electronic transfer systems, continue to be identified as high-risk.
- The return of foreign terrorist fighters remains a potential threat, especially those with combat experience who could re-establish links with extremist networks and facilitate FT .

Risk reduction factors:

- Stable security situation in Serbia from 2021 to 2023
- Ongoing investigations, arrests and strong state efforts to combat terrorism
- Proactive law enforcement, international cooperation and the seizure of illicit assets from organized criminal groups involved in migrant smuggling have been key in reducing any hypothetical FT risks that could be associated with these activities.
- Structured repatriation actions for foreign terrorist fighters , the detention of key returnees, and effective asset freezing measures help mitigate the risk. Continuous monitoring of these individuals shows no immediate signs of re-engagement in terrorist activities, although vigilance is maintained .
- Special assessments and measures regarding high-risk sectors after the 2021 NRA (e-money and payment institutions).

The sectoral overview of FT risks in Serbia based on the 2024 NRA is as follows:

2018	2021	2024
high:	**high:**	**high:**
2018	**2021**	**2024**
medium high: Payment institutions	**medium high:**	**medium high:**

Public postal operator Banks		
2018	**2021**	**2024**
medium: NPOS	**medium:** Electronic money institutions Payment institutions	**medium:** Payment institutions Exchange offices Public postal operator Freelancers in the IT sector NPOs
2018	**2021**	**2024**
medium low :	**medium low :** Public postal operator Exchange offices NPOs	**medium low :** Tourism and hospitality sector Postal services Accountants
2018	**2021**	**2024**
low :	**low :** VASPS Real estate agents Banks	**low :** Public notaries Banks VASPs lawyers Real estate agents Games of chance Financial leasing Life insurance Broker-dealers and investment funds Private pension funds Factoring company auditors Higher education institutions

From the aspect of terrorist financing misuse, there are no identified sectors that are at high or medium-high risk. The medium risk category includes payment institutions and exchange offices. The low to medium risk category includes banks and VASPs. All other sectors are at low risk, but some of them are more susceptible to misuse for terrorist financing purposes.

Since 2018, there has been a significant change in the risk classification of individual sectors, and there are no longer any sectors in the medium-high category. On one hand, this is based on an overall change in the approach to applying the World Bank methodology, due to the greater weight given to preventive measures.

Moreover, there were a number of key improvements in the AML/CFT system after the ICRG process (i.e. for *removal from the FATF grey list)* , which concerned the entire AML/CFT system , and which resulted in an average reduction in FT risk across all sectors:

- o A new supervisory approach has been established in the NPO sector;
- o The authorities have increased their engagement in the NPO sector;
- o A new law on targeted financial sanctions (Law on the Freezing of Assets..) was adopted ;
- o The criminal offence of FT has been amended ;

Also, in the meantime, the banking sector has made significant progress in implementing AML/CFTmeasures , and vulnerabilities have been reduced.

1. High-risk sectors

There are no identified high-risk sectors for terrorist financing in Serbia.

2. Medium risk sectors

These sectors have been identified as having moderate potential for terrorist financing due to business vulnerabilities or insufficient regulatory oversight.

- **Payment institutions:** Vulnerable due to lack of ongoing customer relationships and limited access to identification data of third clients involved in the transaction.
- **Exchange offices: Participation** in the trade of gold, or jewelry, in quantities that deviate from the usual sales of individuals.
- **Freelancers and the IT sector:** Potential use of technological expertise to create or support online content that promotes terrorism.

3. Low to medium risk sectors

These sectors have lower risk, but certain activities make them susceptible to TF abuse.

- **Tourism and hospitality:** Abuse through false or unused reservations and non-transparent payment methods for the services.
- **Postal operators:** Risk of transporting prohibited items or cash transactions with limited recipient identification.
- **Accountants and tax advisors:** Potential abuse through manipulation of financial data for fictitious or suspicious transactions.
- **Banking sector:** Possible abuse of cash loans and money transfers, especially by foreign nationals from high-risk areas.

- **Non-profit organizations:** Recognized vulnerability due to potential abuse in fundraising, transfers of funds, and spending in ways that are inconsistent with statutory objectives.

4. Other

While these sectors are generally low-risk, some are more prone to exploitation based on the nature of their services.

- **VASPs :** While no cases of abuse have been reported in Serbia, global trends show vulnerability to the misuse of cryptocurrencies for terrorism.
- **Lawyers:** Subject to verification of real estate contracts and other high-value transactions with potential terrorist connections.
- **Merchants:** Can be used to purchase goods with possible terrorist use, such as survival equipment, medical supplies, and specialized technical goods.
- **Real estate agents :** Potential abuses in the sale or lease of property by individuals from high-risk areas.
- **Gambling operators**: Potential abuse in online gambling through anonymous accounts and fast money transfers, often linked to digital payment platforms.
- **Financial leasing service providers:** Can be used to finance dubious assets that are out of proportion to typical business activities.
- **Life insurance sector:** Risk of paying large premiums for terrorist financing, especially when third clients are involved.
- **Broker-dealer companies:** Possible abuse in handling investments of foreign entities associated with high-risk areas.
- **Notaries:** The risk of facilitating real estate transactions and contracts involving suspicious entities without sufficient due diligence.
- **Higher education institutions:** Abuse by foreign students to extend residence permits without legitimate educational engagement .

FINANCING RISK ASSESSMENT

Serbia has conducted two risk assessments of PF, in 2021 and 2024 respectively, both as part of a comprehensive national risk assessment exercise and led by the PF subgroup , appointed by the Coordination Body

The system of export controls for arms, military equipment and dual-use goods in Serbia mitigates the risks of financing nuclear proliferation through a strong legal and institutional framework aligned with EU standards. This includes a three-stage process: registration with the Ministry of Internal and Foreign Trade, licensing based on strict criteria to ensure compliance with national and international obligations, and supervision by Customs and relevant ministries to prevent unauthorized diversion. These export control authorities have dealt with specific cases and have thus confirmed their ability to address potential threats.

In the reporting period, the APML processed 5,080 suspicious activity reports (SARs) , none of which related to PF. From 2021 to 2023, six specific cases were investigated in which a connection to PF was suspected, but the suspicions were not confirmed. The system for asset freezing in Serbia has proven to be very operational and efficient, as evidenced by its resolution of various cases, including "false positives" and the application of freezing measures based on domestic terrorist lists. The ability of the system to quickly identify and manage these cases demonstrates its robustness and practical functionality. This operational efficiency suggests that the system would have responded effectively if there had been direct PF cases in Serbia involving individuals on the UN Security Council PF sanctions lists .

Based on an analysis of materiality, threats, vulnerabilities, export control practices, and the effectiveness of controls to prevent PF , the Serbian authorities have concluded that the country is not prone to a number of PF risk scenarios .

Regarding *materiality*, Serbia does not possess the characteristics described by the FATF in its Guidance on PF, which are characterized by a high-risk profile from the PF , e.g. being a large financial center with extensive international trade links and a large volume of cross-border transactions. The country's financial system is relatively isolated from larger global financial flows. The banking sector occupies a dominant position in the Serbian financial system and is almost a monopoly in servicing international transactions, which gives it greater materiality in terms of the PF compared to other sectors.

In terms of *threat* , the assessment considers it unlikely that Serbia will be used for complex or systemic proliferation financing activities, whereby the country's financial infrastructure would be used to finance proliferation activities taking place elsewhere around the world. At the same time, such WMD activities are not ruled out and are still considered possible in the form of sporadic, small-scale attempts, as confirmed by suspicious non-WMD operations identified by the authorities. The following are identified as possible key features of such activities, taking into account the results of transaction monitoring by the competent authorities:

- *Unusual one-off transactions* : Transactions that are inconsistent with the typical financial behavior of a customer, particularly large or complex transactions that are inconsistent with the normal business activities of an individual or entity, may signal an attempt to exploit the Serbian financial system for the purposes of ML/TF . This is particularly relevant for transactions involving foreign persons with no clear ties to Serbia.
- *Use of shell companies or complex corporate structures:* The involvement of shell companies, especially those with unclear ownership structures or newly formed entities, in financial transactions may indicate efforts to conceal the true nature of the transaction. This is a red flag when such companies are used in one-off deals or transactions involving dual-use goods or other sensitive items.

- *Transactions involving high-risk jurisdictions* : Financial transactions involving countries known to be involved in proliferation activities are significant red flags. This includes transfers of funds to or from these jurisdictions, especially when the purpose of the transaction is unclear or does not match the profile of the clients involved.
- *Involvement of non-resident individuals or entities* : The involvement of non-resident individuals or entities in financial transactions within Serbia, particularly those with no apparent business or personal ties to the state, could suggest an attempt to exploit Serbia's financial system for ML/TF .
- *Sudden changes in business activity* : A Serbian company or financial institution that suddenly engages in activities involving high-value goods, dual-use technologies, or significant cross-border transactions, especially when there is no prior history of such activity, may indicate an attempt to use the company or institution as a conduit for PF

There is a reduced direct threat from PF that may involve the procurement of WMD materials in Serbia given the country's limited dual-use industry capacity, combined with strict export control measures and a rigorous licensing process. However, taking into account certain non-PF case scenarios that have occurred in the past, the following risk criteria have been identified:

- *Disproportionate prices of goods:* When the purchase or sale price of dual-use or military goods is significantly higher or lower than the market value, potentially indicating attempts to justify the transaction under questionable circumstances (e.g., motivation of a foreign partner for long-term business).
- *Unusual trade routes or excessive transportation costs:* When export declarations include unusual trade routes that significantly increase transportation costs, such as the route of goods through Serbia rather than directly to the final destination, which may suggest an intent to conceal the true origin or destination of the goods.
- *Exports to high-risk jurisdictions:* Transactions involving countries or entities designated for low levels of transparency, particularly when the purpose, storage and end-use of large quantities of military equipment are unclear or contrary to the needs of the destination country.
- *End-user or foreign partner with a suspicious background:* Cases where due diligence reveals that the end-user or foreign partner has a history of criminal convictions related to illegal trade practices or is subject to trade prohibitions.
- *Purchase of old or surplus military equipment by wealthy nations:* Export licensing requirements involving wealthy nations purchasing obsolete military equipment, where there is no obvious strategic reason for purchasing older items over more modern alternatives, raising questions about the intended use or destination of these goods.

Sectors where the risk of PF is moderate include banks, real estate agents, accountants, tax advisors, lawyers and gambling, while other sectors are considered to carry low risks.

The probability of violations in the banking sector is significantly reduced based on the implemented preventive measures, non-compliance is not reduced (remains neutral) which is the intermediate result of successful measures and remaining shortcomings in the regulation and implementation of measures to prevent FPF ; and avoidance is significantly reduced due to the implemented comprehensive preventive measures. Therefore, for the banking sector, the overall moderate risk assessment is primarily caused by high materiality considerations and some non-compliance issues.

For other sectors in the moderate risk category, materiality considerations do not carry the same weight as for the banking sector, however, issues related to the likelihood of violations and non-compliance are more significant.

Taking into account the multivariate threat, vulnerability and materiality analysis, the PF risk assessment indicates a specific scenario that has a certain (albeit medium-low) probability in the Serbian context, which includes rare, one-off transactions through the banking sector by legal entities engaged in re-export business, with concealment of beneficial ownership, deficiencies in the so-called CDD process (i.e. the application of KYC measures), links with high-risk foreign jurisdictions, and money laundering through trade as a camouflage.

Sectoral Risk Matrix 2024

--	High risk
Sector 1: Banks **Sector 9: Real estate agents** **Sector 10: Accountants and tax advisors** **Sector 11: Lawyers** **Sector 13: Games of chance**	Medium risk
Sector 2: VASPs **Sector 3: Payment operators (including e-money and postal operators)** **Sector 4: Exchange offices** **Sector 5: Brokers/dealers, investment funds** **Sector 6: Insurance** **Sector 7: Financial leasing** **Sector 8: Voluntary pension funds** **Sector 12: Notaries**	Low risk

Key points of conclusion	Impact on the probability of PF
At the same time, the TFS in Serbia is effective in identifying direct objectives (targets)	Partial decrease (-2)
Serbia does not have the characteristics of an international financial center.	Big decrease (-3)
Serbia does not have the characteristics of an international trade hub	Big decrease (-3)
Stronger regional position in finance and trade compared to some Western Balkan countries	Partial increase (+1)
The banking sector's overwhelmingly materially important position in the financial system and its near monopoly on international transactions	Big increase (+3)
The secondary position of other sectors from the point of view of materiality in the context	Big decrease (-3)
Likely threat from PF actors conducting smaller and sporadic/infrequent transactions related to PF	Small increase (+1)
Unlikely threat from systemic PF through sophisticated networks with a financial operational base in Serbia	Partial decrease (-2)

Risk-based approach

Money laundering and terrorist financing risk is the risk of negative effects on the financial result, capital or reputation of the obliged entity, due to the use of the obliged entity (direct or indirect use of a business relationship, transaction, service) for the purpose of money laundering and/or terrorist financing .

The work of accountants is one of the key levers of criminal structures in the process of money laundering because, after a criminal act has been committed, it is necessary to create the appearance of legality for certain transactions through bookkeeping. Hiring the accounting sector is very attractive to potential money launderers because every accounting document submitted for posting, if it is formally correct, will be posted regardless of whether business changes have occurred or not. Accountants can be abused for the purpose of laundering illegally acquired money through recording fictitious income, i.e. income generated from non-existent business grounds, falsely inflated invoices; through posting inflated invoices, when products and services are invoiced at unrealistically high prices, which shows inflated income and profit, and creates a false image of the success of legal entities' business operations; through the preparation of false income tax returns; through the provision of advice for the purpose of tax evasion; through the establishment and management of companies and charities, thereby helping to create complex ownership structures in order to conceal a complex money laundering scheme; through the misrepresentation of data in financial statements, etc. In addition to the above, accountants can also provide tax consulting services, which is also attractive to "money launderers", because accountants can provide them with expert advice regarding tax regulations.

The risk of money laundering and terrorist financing arises particularly as a consequence of failure to comply with the obliged entity's operations with the Law, regulations and internal acts regulating the prevention of money laundering and terrorist financing, or as a consequence of mutual inconsistency of internal acts regulating the actions of the obliged entity and its employees in relation to the prevention of money laundering and terrorist financing.

Money laundering and terrorist financing is a real and serious problem that obliged entities must confront so as not to inadvertently or otherwise encourage or incite it.

The problem of money laundering must be approached as a complex phenomenon, in order to avoid its negative effects. The "path" of dirty money is not easy to spot and recognize, which certainly makes it difficult to take timely and effective measures to detect, prevent and combat it. Money laundering takes on new forms every day, using various methods and means.

It is essential that obliged entities adopt a risk-based approach to identifying, assessing and understanding money laundering and terrorist financing risks, in order to focus their resources where the risks are greatest and thereby implement appropriate risk mitigation measures.

Key elements of a risk-based approach:

Risk detection and assessment	Disclosure of the risks of money laundering and terrorist financing faced by the obliged entity, considering the clients, services, countries of operation, also taking into account publicly available information on the risks and typologies of money laundering and terrorist financing

Risk management and mitigation	Identifying and implementing measures to efficiently and effectively mitigate and manage the risk of money laundering and terrorist financing
Ongoing monitoring	Defining policies and procedures for monitoring changes in money laundering and terrorist financing risks
Documentation	Documenting risk assessments, policies and procedures for monitoring, managing and mitigating money laundering and terrorist financing risks

Risk analysis (assessment) at the obliged entity level (self-risk assessment)

In the process of developing a risk analysis in relation to its entire business, the obliged entity assesses the likelihood that its business will be used for that purpose. The risk analysis in relation to the obliged entity's entire business aims to identify the obliged entity's exposure to the risk of money laundering and terrorist financing and PF segments of the obliged entity's business that should be given priority in undertaking activities to effectively manage this type of risk.

The obliged entity is required to carry out a risk assessment at the obliged entity level (self-risk assessment) **once a year , no later than March 31 of the current year for the previous year.** based on the analysis of the self-assessment criteria below .

A prerequisite for developing a risk analysis at the obliged entity level is a developed risk analysis of all clients with which the obliged entity has established a business relationship, which, in addition to taking into account the results of the national risk assessment and mandatory legal provisions, includes geographical risk, customer risk and service risk, and in the case of factoring companies, transaction risk, the assessment criteria for which are given in a separate section of these Guidelines.

When assessing risk at the obliged entity level, the obliged entity is required to take into account at least:

- results of the national risk assessment, i.e. threat risk and sectoral vulnerability. According to the results of the national risk assessment from 2024, the accounting sector is assessed as medium- high vulnerable and has high exposure to money laundering threats and the factoring sector is assessed as medium-low vulnerable and has a medium exposure to money laundering threats . Also, when self-assessing the risk, the obliged entity must take into account the riskiness of the form in which the obliged entity is organized, according to the results of the national risk assessment, which are listed below;

- whether there are products or services that the obliged entity offers in its business that could be abused ;
- the size of the obliged entity , whether the obliged entity has a complex ownership structure, the number of employees at the obliged entity directly responsible for performing tasks related to preventing money laundering and terrorist financing in relation to the total number of employees, the number of employees who are in direct contact with clients, the method of organizing work and responsibilities, the dynamics of hiring new employees, the quality of training, etc .;
- total number of clients;
- number of clients with complex ownership structure;
- number of clients by legal form - according to the results of the 2024 national risk assessment, limited liability companies and sole proprietorships (businesses) represent forms of business entities with a high level of exposure to money laundering risk, associations and cooperatives represent a medium level of risk, and other forms of legal entities represent a low level of risk exposure (and the analysis of the participation of legal entities in money laundering cases indicates the fact that legal entities, especially small LLCs, have a central role in laundering illegal income; money is most often laundered through fictitious transactions, in which false invoices and documents are used, and business activity is simulated ; such entities are often under the control of organized criminal groups and are used for the movement and integration of dirty money into the legitimate financial system) .
- assessment of the obliged entity's exposure to cross-border threats (number of clients that are residents and number of clients that are non-residents, number of clients whose beneficial owners are domestic citizens and number of clients whose beneficial owners are foreign citizens, and if there are beneficial owners who are foreign citizens, information on which country they are from);
- the level of risk of its clients (number of low, medium and high risk clients, especially taking into account the number of offshore legal entities, officials and clients who were not physically present when establishing the business relationship);
- number of clients with suspicious activities/transactions;
- number of suspicious activities/transactions identified in internal reports and number of suspicious transactions reported to the APML.

Based on the above criteria, as well as the measures it takes to mitigate the risk of money laundering and terrorist financing, the obliged entity assesses its overall exposure to the risk of money laundering and terrorist financing as **low risk, medium risk or high risk** .

The obliged entity is not expected to determine whether a criminal act of money laundering or terrorist financing has been committed. The primary task of the obliged entity is to ensure that all necessary data is available in relation to the knowledge and monitoring of the business of its clients, to assess whether and to what extent certain patterns of behavior can be linked to a criminal act, and to take all necessary measures and report suspicious activities in accordance with the Law,

while the APML and the investigative authorities further conduct the necessary procedures in a given case, in order to determine whether or not a criminal offence has been committed.

Analysis (assessment) at the level of a business relationship (a client)

As stated above, the obliged entity performs the risk assessment at the business relationship (party) level taking into account:

- Results of the national risk assessment (if the client is an obliged entity, the client is obliged to take into account the level of threat and sectoral vulnerability of the sector to which the client belongs , as well as the riskiness of the legal form in which the client is organized, regardless of whether the client is a client obliged to the Law);
- mandatory provisions of the Law (The Law prescribes cases when the obliged entity is required to classify a client as high risk and to apply enhanced CDD in relation to it) ;
- Guidelines of the Administration for the Prevention of Money Laundering (geographic risk, customer risk, service risk, for factoring company transaction risk is added, the criteria for which are given in a separate section of these Guidelines).

The risk assessment of a customer is carried out not only when establishing a business relationship with a customer, but also throughout the entire duration of the business relationship, and the level of risk may change. For example, a certain business relationship with a customer may initially be assessed as low-risk, and then circumstances may arise that will increase that risk, and vice versa. This does not apply to cases that are classified as high-risk under the Law and to which enhanced actions and measures of knowing and monitoring the customer must be applied (e.g. when the customer is an official, when the customer is not physically present during the identification and verification of identity, when the client or a legal person appearing in the client's ownership structure is an offshore legal person, when establishing a business relationship or carrying out a transaction with a client from a country that has strategic deficiencies in the system for preventing money laundering and terrorist financing).

The degree of risk at the level of the business relationship (the client) and the type of CDD measures

Based on the risk assessment performed for each group or type of client, i.e. business relationship, the service provided by the obliged entity within the scope of its activity, i.e. transaction - the obliged entity, in accordance with the Law, classifies the client into one of the following risk categories:

– the category of **low risk** of money laundering and terrorist financing and then applies at least least simplified CDD;

– the category of **medium risk** of money laundering and terrorist financing and then applies at least general CDD;

– the category of **high risk** of money laundering and terrorist financing and then applies enhanced CDD .

The obliged entity may also provide for additional risk categories through internal acts.

International standards and the Law allow the obliged entity to, depending on the level of risk of money laundering and terrorist financing, implement three types of customer due diligence actions and measures - from simplified to enhanced.

- ***General CDD measures*** include establishing and verifying its identity and the identity of the beneficial owner, obtaining and assessing information on the purpose of the customer's business relationship or transaction, as well as regularly monitoring its business and checking the compliance of the customer's activities with the nature of the business relationship and the usual scope and type of business of the customer.

- ***Enhanced CDD measures***, in addition to general CDD, include: obtaining and assessing the reliability of information on the origin of property that is or will be the subject of a business relationship and additional actions and measures that the obliged entity takes in cases prescribed by the Law, as well as in other cases when it assesses that there is or could be a high level of risk of money laundering or terrorist financing. The obliged entity defines in its internal act which enhanced measures, and to what extent, will be taken in each specific case.

What additional measures the obliged entity will take when it classifies a customer in a high-risk category based on its own risk assessment depends on the specific situation (e.g. if the customer is so assessed due to its ownership structure, the obliged entity may provide in its procedures for the obligation to obtain additional data and the requirement to additionally check the submitted documentation).

The requirement to take enhanced CDD applies in the following cases prescribed by the Law:

a) New technological developments and services

The obliged entity is required to recognize and understand the risks associated with a new or innovative product or service, especially when it involves the use of new technologies or payment methods. New products and new business practices, including new ways of delivering products and the use of new technologies in development (for both new and existing products), especially if they are not clearly understood, may contribute to an increased risk of money laundering and terrorist financing.

When implementing new technological developments and new products or services, the obliged entity is required by law, in addition to general CDD, to apply additional measures to reduce risks and manage the risk of money laundering and terrorist financing (e.g. more frequent monitoring of the customer to determine whether its business operations are as expected, taking into account the knowledge of the customer, its income, etc.).

b) An official (a PEP)

The obliged entity regulates the procedure for determining whether a client or the beneficial owner of a client is an official, a member of the official's close family, or a close associate of an official.

The CDD measures should be a key source of information on whether the client is an official (e.g. information on the client's main occupation or employment). The obliged entity also uses other sources of information that may be useful for identifying the official.

In order to obtain relevant information for identifying the official, the obliged entity undertakes one of the following activities:

- obtains a written statement from the client as to whether they are an official, a close family member of an official, or a close associate of an official;
- uses electronic commercial databases containing lists of officials (e.g. *World-Check, Factiva, LexisNexis*);
- searches publicly available data and information (e.g. the register of officials of the Anti-Corruption Agency);
- forms and uses an internal database of officials (e.g. larger financial groups have their own lists of officials).

The number, or rather the sequence, of the activities disclosed by the obliged entity should enable reliable determination of whether the client or the beneficial owner of the client is an official, a member of the official's close family, or a close associate of the official.

The written statement contains the following information:

- name and surname, date and place of birth, place of permanent/temporary residence and personal identification number/personal identification number of the official establishing a business relationship or carrying out a transaction, or on whose behalf the business relationship is being established or the transaction is being carried out, as well as the type and number of the personal document, name of the issuer, date and place of issue;
- a statement on whether the client is an official according to the criteria set out in the Law (the statement should list all cases provided for by the Law in detail);
- information on whether the official is a natural person who holds or has held a high public office in the state, another state or international organization in the last four years, or whether he is a family member of the official or his close associate;
- data on the period in office;
- data on the type of public function that the official holds or has held in the last four years;
- data on the family relationship, if the client is a member of the official's close family;
- information on the type of business cooperation, if the client is a close associate of the official.

When establishing a business relationship with a client who is an official, a member of the official's close family or a close associate of an official, or whose beneficial owner is one of these persons, the obliged entity shall also apply enhanced CDD. The obliged entity shall also apply these measures when a natural person ceases to perform a public function (former official), for as long as it takes to conclude that that person did not abuse the position he held, and for at least four years from the date of cessation.

The data and documentation obtained in this procedure are kept in the client's file for 10 years from the date of termination of the business relationship.

c) Identification and verification of identity without the physical presence of the client

If, when establishing and verifying the identity, the client or the legal representative, or the person authorized to represent the legal person or foreign legal person, is not physically present at the obliged entity's premises - in accordance with the Law, the obliged entity is obliged, in addition to general CDD, to apply additional measures prescribed by Article 39 of the Law, which relate to obtaining additional documents, data or information, on the basis of which it verifies the client's identity; additional verification of submitted documents or additional confirmation of data about the client; obtaining data on the reasons for the client's absence (it is necessary to attempt to establish additional contact with the client by phone, email, Skype, Viber or in another manner and to collect another identification document for the client).

d) An offshore legal person

In accordance with the Law, the obliged entity is required to establish the procedure by which it determines whether a client or a legal person appearing in its ownership structure is an offshore legal person. In order to determine whether it is an offshore legal person, the obliged entity may use the lists of the IMF, the World Bank or the list of countries that is an integral part of the Regulation on the list of jurisdictions with a preferential tax system ("Official Gazette of the Republic of Serbia", No. 122/12 , 104/18 and 161/20). If, based on the procedure carried out, it has been determined that a client or a legal person appearing in the ownership structure of the client is an offshore legal person, the obliged entity is obliged to take additional (enhanced) CDD measures in accordance with the Law, in addition to general CDD.

e) Countries that do not apply international standards in the field of preventing money laundering and terrorist financing

In accordance with the Law, strategic deficiencies in the system for combating money laundering and terrorist financing of a country relate in particular to 1) the legal and institutional framework of the country, and in particular to the criminalization of money laundering and terrorist financing, customer due diligence measures, provisions regarding data retention, provisions regarding the reporting of suspicious transactions, the availability of accurate and reliable information on the beneficial owners of legal entities and foreign legal entities; 2) the powers and

procedures of the competent authorities of those countries regarding money laundering and terrorist financing; 3) the effectiveness of the system for combating money laundering and terrorist financing in eliminating the risk of money laundering and terrorist financing.

When establishing a business relationship or carrying out a transaction when a business relationship has not been established with a client from a country that has strategic deficiencies in the system for combating money laundering and terrorist financing - the obliged entity is obliged to implement enhanced CDD prescribed by the Law.

- ***Simplified CDD measures*** are undertaken in cases and in the manner prescribed by the Law and the Rulebook on the Methodology for Performing Operations in Accordance with the Law on the Prevention of Money Laundering and Financing of Terrorism and are applied to clients with a low level of risk of money laundering and financing of terrorism. Clients may also be classified in this risk category based on a risk analysis. The obliged entity is required to undertake general CDD, except in the case when the client is a state body, an autonomous province body, a local government unit body, a public enterprise, a public agency, a public service, a public fund, a public institute or a chamber, or a business company whose securities are included in an organized securities market located in the Republic of Serbia or a country in which international standards at the level of European Union standards or higher are applied, and which relate to the submission of reports and the disclosure of data to the competent regulatory body, in which situation the obliged entities are not obliged to determine the beneficial owner of the client. The obliged entity is required to establish an adequate level of monitoring of the client's operations, so as to be able to detect unusual and suspicious transactions. When suspicion arises that money laundering or terrorist financing is involved in respect of a client or transaction to which these measures have been applied, the obliged entity is required to conduct an additional assessment and possibly apply enhanced CDD.

Ongoing monitoring

Frequency of customer monitoring by risk category

After the obliged entity classifies the clients according to the degree of risk into categories:

- low level of risk of money laundering and terrorist financing;
- medium level of risk of money laundering and terrorist financing;
- high level of risk of money laundering and terrorist financing,

The obliged entity applies CDD measures in the course of the business relationship, with a frequency and intensity in accordance with the assessed risk and changed circumstances in relation to the customer, so that:

- clients classified as low risk are monitored at least once every two years;
- Clients classified as medium risk are monitored at least once a year;

- Clients classified as high risk are monitored at least once every six months.

Documentation

A risk-based approach also requires documentation of the risk assessment, as well as the existence of appropriate internal documents to determine starting points and implement adequate measures and procedures.

Internal acts

In accordance with the provisions of the Law, the obliged entity is obliged to adopt and implement appropriate internal acts that, for the purpose of effective management of the risk of money laundering and terrorist financing, will include all actions and measures for the prevention and detection of money laundering and terrorist financing defined by the Law, by-laws adopted on the basis of the Law and these Guidelines. The obliged entity is obliged to take into account the identified risks of money laundering and terrorist financing through internal acts, whereby these acts must be proportionate to the nature and scope of operations, as well as the size of the obliged entity, and must have the approval of a member of the senior management. The obliged entity is obliged to ensure the implementation of these internal acts by establishing appropriate procedures and internal control mechanisms.

The obliged entity is obliged to regulate in particular through internal acts:

- the process of developing a money laundering and terrorist financing risk analysis;
- procedures and mechanisms for detecting suspicious transactions and/or clients, as well as the manner in which employees act upon recognizing such transactions and procedures for submitting information, data and documentation at the obliged entity level;
- determining the persons responsible for carrying out the obligations under the Law - the AML/CFT compliance officer and his/her deputy, as well as ensuring the conditions for their work [1];
- measures and actions to monitor the customer's operations that will be undertaken, or carried out, in accordance with the customer's risk category in the course of the business relationship, conditions for changing its status according to the level of exposure to the risk of money laundering and terrorist financing, and periods of monitoring customers according to the level of risk;

[1] The obliged entity is obliged to submit data on the personal name and job title of the authorized person, his/her deputy and the member of the top management responsible for the implementation of the Law (notification or decision on appointment with the specified data), as well as any changes to such data, to the APML no later than 15 days from the date of appointment.

- determining the acceptability of the client according to the level of risk of money laundering and terrorist financing when establishing a business relationship and in the course of it;
- determining the risk category of the customer, services, transactions according to risk factors in relation to the risk of money laundering and terrorist financing;
- the procedure for implementing customer due diligence actions and measures, and regular monitoring of its operations in accordance with the established risk category, including checking the compliance of the customer's activities with the nature of the business relationship and the usual scope and type of its operations, as well as any possible change in its risk category;
- the procedure for implementing enhanced CDD, when the customer is high-risk under the Law itself or based on a risk analysis, and in particular the procedure for determining whether the customer or its beneficial owner is an official, as well as the procedure for determining whether the customer or a legal person appearing in the customer's ownership structure is an offshore legal person;
- the procedure for regular internal control of the implementation of obligations under the Law, in accordance with the Law and the preparation of an annual report on the internal control performed and measures taken after that control no later than March 15 of the current year for the previous year with the content prescribed by the Rulebook ;
- the procedure for implementing regular professional education, training and advanced training of employees in accordance with the annual professional education, training and advanced training program for those performing tasks related to the prevention and detection of money laundering and terrorist financing, which is compiled by the end of March for the current year with the content prescribed by the Rulebook [2];
- record keeping, protection and storage of data from those records .

An integral part of the internal acts is a list of indicators for identifying persons and transactions with regard to which there are reasons to laundering or terrorist financing or proliferation financing , as well as a list of indicators for identifying suspicious activities related to terrorist financing, which contain all indicators developed by the Administration for the Prevention of Money Laundering and published on its website. (http://www.apml.gov.rs/srp49/dir/Indikatori.html). Also, obliged entities can supplement the list of indicators according to trends and typologies of money laundering known to them, as well as according to circumstances arising from the obliged entity's business operations.

The list of indicators for identifying suspicious transactions is a starting point for the obliged entity when identifying suspicious activities of a client. Namely, in the process of determining the existence of elements for qualifying a certain transaction as suspicious, the indicators compiled by the APML as a supervisory authority should be taken into account. However, a transaction may be suspicious without being classified under any indicator. In that

[2] In addition to the above, the obliged entity is obliged to prepare an official note on the training conducted, the content of which is also prescribed by the Rulebook.

case, the obliged entity should consider the broader context, because the obliged entity knows his or her clinet best and in that sense, the obliged entity may assess that the transaction is suspicious even though it cannot be classified under any indicator published by the APML. On the other hand, if a transaction can be characterized as suspicious based on an indicator of the APML, this does not mean that the obliged entity must immediately report the transaction as suspicious to the APML, but rather that the client should be monitored more closely and, depending on the circumstances, assess whether a report should be made to the APML. The report of suspicious activity by the client is made on a form that is an integral part of the Rulebook.

If an employee of an obliged entity who is in direct contact with a client suspects that there is a risk of money laundering and terrorist financing in relation to that client or its transaction, he or she is obliged to prepare an internal written report on this matter and to submit it, within the deadline and in the manner determined by the internal act of that obliged entity, to the person responsible exclusively for the execution of obligations under the Law and other regulations governing the prevention of money laundering and terrorist financing , i.e. AML/CFT compliance officer. This report should contain such data on the client and the transaction that enable the AML/CFT compliance officer to assess whether the client or the transaction is suspicious.

If, based on this report or other information about a risk of money laundering and terrorist financing that he or she directly learns, the AML/CFT compliance officer assesses a transaction as suspicious - that person shall proceed in accordance with the Law, and if he or she does not assess it as such - he or she shall be obliged to make a note of that assessment.

In addition to drafting internal documents, the obliged entity is obliged to document all actions and measures taken towards the client. in accordance with the Law.

Identification of the client, its representative, proxy, beneficial owner, risk analysis of the client, entry of data into records, are carried out when establishing a business relationship with the client and all data and documentation are regularly updated and stored in business documentation. Identification of the client is carried out by inspecting the documentation from the official public register of the client's country of residence or by direct inspection i.e. by inspecting the personal document on whose copies in paper form, i.e. a scanned extract of the personal document in paper form, the date, time and personal name of the person who inspected the document are entered, i.e. a copy of the document in electronic form contains a qualified electronic stamp, i.e. a qualified electronic signature with an associated time stamp. Also, a copy of the documentation, i.e. a scanned extract of the personal document, is also considered a digitized document and a copy of the documentation, i.e. a scanned extract of the personal document can be stored in paper or electronic form.

Also, the obliged entity is obliged to keep data and related documentation in accordance with the Law on the Prevention of Money Laundering and Financing of Terrorism .

SPECIAL PART

A particular part of these Guidelines shall be applied by the obliged entity to whom that part applies, taking into account the specific circumstances relating to the risks .

1. Types of risks for entrepreneurs and legal entities engaged in the provision of accounting services

The risk assessment, within the meaning of these Guidelines, should cover at least the following three basic types of risk: geographical risk, customer risk and service risk that the obliged entity provides within the scope of its activity. In the case of identifying other types of risk, and depending on the specifics of the business - the obliged entity should also include these types of risks in the assessment.

I Geographical **risk** refers to the risk that is conditioned by the geographical area in which the territory of the country of origin of the client, its owner or majority founder, beneficial owner or person who otherwise controls the client's business is located, or in which the country of origin of the person who conducts a transaction with the client is located.

Factors that determine whether a particular country or geographic location poses a higher risk of money laundering and terrorist financing include:

● countries against which the United Nations, the Council of Europe, or other international organizations have applied sanctions, embargoes, or similar measures;

● countries that have been identified by credible institutions (FATF, Council of Europe, IMF, World Bank, etc.) as not implementing adequate measures to prevent money laundering and terrorist financing. Here, special attention is paid to the process - ICRG FATF (International Cooperation Review Group). After each meeting, FATF publishes a list of countries thatdo not have an adequate system for combating money laundering and terrorist financing;

● countries that have been designated by credible institutions (FATF, UN, etc.) as countries that support or finance terrorist activities or organizations;

● countries that have been designated by credible institutions (e.g. the World Bank, IMF) as countries with high levels of corruption and crime.

● offshore legal entities, in accordance with the Law.

The list of countries with strategic deficiencies in their anti-money laundering and counter-terrorist financing systems is published on the website of the APML. The list of countries is based on the following:

1) FATF (*Financial Action Task Force*) statements on countries that have strategic deficiencies in their systems for combating money laundering and terrorist financing and that pose a risk to the international financial system ;

2) FATF statements on countries/jurisdictions that have strategic deficiencies in their anti-money laundering and counter-terrorist financing systems, which have expressed a commitment at

the highest political level to address the identified deficiencies, which have developed an action plan in cooperation with FATF for this purpose, and which are obliged to report on the progress they are making in addressing the deficiencies ;

3) on reports on the assessment of national systems for combating money laundering and terrorist financing by international institutions (FATF and FSRBs such as the Council of Europe MONEYVAL Committee).

Countries that apply standards in the field of preventing money laundering and terrorist financing that are at the level of European Union standards or higher are:

1) EU Member States;

2) Third countries (other non-EU countries) with effective systems for preventing money laundering and terrorist financing, assessed in reports on the assessment of national systems for combating money laundering and terrorist financing by international institutions (FATF) and the so-called regional bodies that operate on the model of the FATF, such as MONEYVAL);

3) Third countries (other non-EU countries) that have been identified by credible sources (for example *Transparency International*) as having low levels of corruption or other criminal activities;

4) Third countries (other non-EU countries) which, based on credible sources, such as reports on the assessment of national systems for combating money laundering and terrorist financing by international institutions (FATF and FSRBs), published reports on the progress of that country following the report, have in place the obligations prescribed by law to combat money laundering and terrorist financing in accordance with the FATF recommendations and effectively implement those obligations.

The increased risk of money laundering and terrorist financing is posed by clients that have a contractual relationship and carry out business activities with persons from offshore. For example, a high-risk client will be a client that has a service transaction with a client that is headquartered in a country with a preferrential tax system. This part was also pointed out by the country's risk assessment, when looking at case studies, money laundering convictions and typologies of criminal group behavior, and especially when it comes to organized criminal groups, the obliged entity must be aware of the assessed threats and carefully analyze relationships where offshore territories and countries in the region appear as a geographical element.

Namely, although certain countries apply the standards, this does not mean that they will immediately be placed in the group of countries, according to the obliged entity's risk assessment, at low risk, but rather the typology of behavior and money laundering cases must be taken into account, which have indicated a higher risk of certain countries, which the obliged entity must approach with due care.

A client that has a contractual relationship with a client from the region may have a low risk of money laundering. For example, a client that trades goods with a client from a country in the region may be low-risk because there is an economic justification for such a relationship.

Or, for example, a low-risk party may be one that is registered for the trade of goods and where, upon further monitoring of the business, it is concluded that all transactions with suppliers and customers are related to the business it performs and are not registered at destinations that would indicate a possible increased risk.

II Client risk - The obliged entity determines the approach to counterparty risk based on its own experience and knowledge of business rules. However, it is obliged to apply the restrictions set out in the Law and other regulations governing the prevention of money laundering and terrorist financing.

1) The following unusual activities may indicate increased risk:

- when establishing a business relationship with the obliged entity, the client avoids to appear in person and insists on indirect contact;

- the client, without any particular reason, demands the business to be done quickly, regardless of the higher costs that such action will cause;

- the client pays for goods or services that do not correspond to the description of their business;

- a client offers money, gifts or other benefits in return for a business operation that is suspected of not being fully compliant with regulations;

- the client wants to convince the accountant that it is not necessary to fill out or attach any of the required documents; avoids submitting the required documentation or the obliged entity has suspicion whether the submitted documentation is accurate or complete; does not know where the business documentation is kept;

- the client frequently changes its accountants;

- the client has no employees or business premises, which is not proportionate to the volume of business; it makes frequent changes to its name, registered office, ownership structure, etc.

2) clients where, due to their structure, legal form or complex and unclear relationships, it is difficult to determine the identity of their beneficial owners or the persons who manage them, such as, in particular:

- foundations, trusts or similar entities under foreign law,

- charitable and non-profit organizations,

- offshore legal entities with an unclear ownership structure and not established by a company from a country that applies standards in the field of preventing money laundering and terrorist financing that are at the level of the standards prescribed by the Law;

3) agricultural holding ;

4) clients that carry out activities characterized by large turnover or cash payments (restaurants, gas stations, exchange offices, casinos, flower shops, dealers in precious metals, cars, works of art, transport companies for goods and passengers, sports clubs, construction companies);

5) officials, in accordance with the Law;

6) private investment funds;

7) clients whose offer to establish a business relationship was rejected by another obliged entity, i.e. persons with a bad reputation;

8) clients whose source of funds is unknown or unclear, i.e. which the client cannot prove;

9) the client has lived abroad for a long time, without proof of employment, and is depositing a large sum of money to open a legal person engaged in the provision of services (catering services, consulting services, marketing services, event management services, etc.);

10) clients suspected of not acting on their own behalf, i.e. carrying out instructions from a third party;

11) establishment of companies or foreign legal entities as single-member limited liability companies, with a minimum share capital, registered for the activities of non-specialized wholesale trade, consulting, marketing and IT services and activities related to construction, including the drafting of articles of association and their notarization;

12) change in the ownership and management structure of companies or foreign legal entities established as single-member limited liability companies, with minimal share capital, with fewer than three employees and disproportionately high revenues generated in a short period of time, including the preparation of acts on status changes and their notarizations;

13) unemployed individuals who generate large turnover on their accounts ;

14) disproportionate prices of goods - where the purchase or sale price of dual-use goods or military goods is significantly higher or lower than the market value, potentially indicating attempts to justify the transaction under dubious circumstances (e.g. motivation of a foreign partner for long-term business) ;

15) unusual trade routes or excessive transport costs - when export declarations include unusual trade routes that significantly increase transport costs, such as the route of goods through Serbia, rather than directly to the final destination, which may suggest an intention to conceal the true origin or destination of the goods ;

16) and shipments to high-risk jurisdictions that include countries or entities designated for low levels of transparency, especially when the purpose, storage and end-use of large quantities of military equipment are unclear or contrary to the needs of the destination country.

17) end-user or foreign partner with a suspicious background - cases in which due diligence reveals that the end-user or foreign partner has a history of criminal convictions related to illegal trade practices or is subject to trade prohibitions ;

18) the repurchasing of old or surplus military equipment by wealthy nations - export licensing requirements that involve wealthy nations purchasing obsolete military equipment, where there is no obvious strategic reason for purchasing older items over more modern alternatives, leading to questions about the intended use or destination of these goods.

We would also like to point out that if the obliged entity assesses that the offshore legal person party or a legal person appearing in the ownership structure of the offshore legal person party has a complex ownership structure (such as a large number of legal entities in the founding

structure, of which persons with a significant share in the founding capital are registered in offshore destinations and when it cannot be easily determined who the beneficial owner of those legal entities is), the obliged entity is obliged to obtain a written statement from the beneficial owner of the client or the client's representative on the reasons for such a structure, as well as to consider whether there is a basis for suspicion that money laundering or terrorist financing is involved and to make an official note on this, which he shall keep in accordance with the Law.

The obliged entity must pay particular attention if it enters into a business relationship with a client which deals with: buying and selling real estate, investments, construction activities, real estate construction, frequent trade in goods and services without supporting documents, investments in securities.

The situations described in the national risk assessment indicate a higher risk in the above-mentioned activities. All the activities listed, and identified by the client call for a greater attention and risk assessment, as well as the need to monitor and assess the activities of these persons more frequently.

III The service risk includes the following:

1) business that significantly differs from the usual business of a client engaged in a similar activity, as well as business that does not have economic justification (e.g. frequent trading in securities when purchases are made by depositing cash into designated accounts, and soon afterwards selling below price - so-called trading in securities with a planned loss, unexpected repayment of a loan before the due date or within a short period from the date of loan approval, withdrawal of funds from the individual account of a member of a voluntary pension fund within a short period after their payment) ;

2) transactions carried out by the client in amounts slightly lower than the amounts prescribed as reporting limits in accordance with the Law;

3) loans to legal entities, especially loans from founders from abroad to legal entities in the country that do not have economic justification;

4) payment for consulting, management and marketing services, as well as other services for which there is no determinable value or price on the market;

5) payment for goods and services to the client's partners originating from offshore destinations, and the documentation clearly shows that the goods originate from surrounding countries;

6) procurement of goods from countries where those goods are not produced;

7) the frequency of transactions based on advance payment for the import of goods or the provision of services where it is not certain that the goods will actually be imported or the service performed;

8) increased or decreased invoices for goods or services; multiple invoicing; multiple payments - payments for the same goods or services (for the same product purchased or service performed, payment is made multiple times to the same or a different supplier); abuse of write-offs of goods

(the customer often and to a greater extent writes off part of the sold goods due to various factors - force majeure, perishability, loss of goods during transport, inadequate storage, breakage, etc. - which in reality did not even occur);

9) the customer makes payments for goods and services through electronic banking, and does not have documentation for it;

10) the client makes life insurance payments in large lump sums for all employees;

11) the client places a disproportionately high deposit amount (e.g. 100%) with several banks as collateral for obtaining a credit or loan;

12) business relationships or transactions arising from re-export transactions;

13) frequent or large-scale transactions related to the payment of winnings from online games of chance;

14) crowdfunding;

15) business relationships or transactions related to digital assets that include large-value transactions in stable digital assets, transactions that are carried out outside a payment account – such as P2P transactions, as well as transactions where it is difficult or impossible to determine the origin of funds;

16) business relationships or transactions involving providers of services related to digital assets in jurisdictions that do not apply international standards for the prevention of money laundering and terrorist financing in the field of digital assets;

17) business relations or transactions with a person involved in the trade of weapons, military equipment or dual-use items;

18) business relationships or transactions with a person involved in the trade of gold and works of art;

19) transactions related to the legalization of constructed real estate ;

20) unusual one-off transactions that are not consistent with the typical financial behavior of the client, especially large or complex transactions that are not consistent with the normal business activities of the individual or entity, may signal an attempt to exploit the financial system of Serbia for the purposes of PF (this is particularly relevant for transactions involving foreign persons who have no clear ties to Serbia);

21) The use of shell companies or complex corporate structures - more often shell companies, especially those with unclear ownership structures or newly formed entities, in financial transactions may indicate efforts to conceal the true nature of the transaction. This is a red flag when such companies are used in one-off deals or transactions involving dual-use goods or other sensitive items ;

22) Transactions involving high-risk jurisdictions - financial transactions involving countries known to be involved in proliferation activities are significant red flags. This includes transfers of funds to or from these jurisdictions, particularly when the purpose of the transaction is unclear or does not match the profile of the clients involved ;

23) the increased use of non-resident individuals or entities in financial transactions within Serbia, especially those with no obvious business or personal ties to the state, could suggest an attempt to exploit the Serbian financial system for PF;

24) sudden changes in business activity - a domestic company or financial institution suddenly engaging in activities involving high-value goods, dual-use technologies, or significant cross-border transactions, especially when there is no prior history of such activity, may indicate an attempt to use the company or institution as a conduit for ML/TF .

2. Types of risk in factoring companies

Risk assessment, within the meaning of these Guidelines, should cover at least four basic types of risk: geographical risk, customer risk, transaction risk and service risk .

In the event of identifying other types of risks, due to the specific feature of purchasing receivables i.e. factoring, the obliged entity should also include those types of risks.

I Geographic risk - Factors that determine whether a particular country or geographic location poses a higher risk of money laundering and terrorist financing include:

● countries against which the United Nations, the Council of Europe, or other international organizations have applied sanctions, embargoes, or similar measures;

● countries that have been identified by credible institutions (FATF, Council of Europe, IMF, World Bank, etc.) as not implementing adequate measures to prevent money laundering and terrorist financing. Here, special attention is paid to the process - ICRG FATF (International Cooperation Review Group). After each meeting, FATF publishes a list of countries thatdo not have an adequate system for combating money laundering and terrorist financing;

● countries that have been designated by credible institutions (FATF, UN, etc.) as countries that support or finance terrorist activities or organizations;

● countries that have been designated by credible institutions (e.g. the World Bank, IMF) as countries with high levels of corruption and crime.

● offshore legal entities, in accordance with the Law.

The list of countries with strategic deficiencies in their anti-money laundering and counter-terrorist financing systems is published on the website of the APML. The list of countries is based on the following:

1) FATF (*Financial Action Task Force*) statements on countries that have strategic deficiencies in their systems for combating money laundering and terrorist financing and that pose a risk to the international financial system ;

2) FATF statements on countries/jurisdictions that have strategic deficiencies in their anti-money laundering and counter-terrorist financing systems, which have expressed a commitment at the highest political level to address the identified deficiencies, which have developed an action

plan in cooperation with FATF for this purpose, and which are obliged to report on the progress they are making in addressing the deficiencies ;

3) on reports on the assessment of national systems for combating money laundering and terrorist financing by international institutions (FATF and FSRBs such as the Council of Europe MONEYVAL Committee).

Countries that apply standards in the field of preventing money laundering and terrorist financing that are at the level of European Union standards or higher are:

1) EU Member States;

2) Third countries (other non-EU countries) with effective systems for preventing money laundering and terrorist financing, assessed in reports on the assessment of national systems for combating money laundering and terrorist financing by international institutions (FATF) and the so-called regional bodies that operate on the model of the FATF, such as MONEYVAL);

3) Third countries (other non-EU countries) that have been identified by credible sources (for example *Transparency International*) as having low levels of corruption or other criminal activities;

4) Third countries (other non-EU countries) which, based on credible sources, such as reports on the assessment of national systems for combating money laundering and terrorist financing by international institutions (FATF and FSRBs), published reports on the progress of that country following the report, have in place the obligations prescribed by law to combat money laundering and terrorist financing in accordance with the FATF recommendations and effectively implement those obligations.

The increased risk of money laundering and terrorist financing is posed by clients that have a contractual relationship and carry out business activities with persons from offshore. For example, a high-risk client will be a client that has a service transaction with a client that is headquartered in a country with a preferrential tax system. This part was also pointed out by the country's risk assessment, when looking at case studies, money laundering convictions and typologies of criminal group behavior, and especially when it comes to organized criminal groups, the obliged entity must be aware of the assessed threats and carefully analyze relationships where offshore territories and countries in the region appear as a geographical element.

Namely, although certain countries apply the standards, this does not mean that they will immediately be placed in the group of countries, according to the obliged entity's risk assessment, at low risk, but rather the typology of behavior and money laundering cases must be taken into account, which have indicated a higher risk of certain countries, which the obliged entity must approach with due care.

A client that has a contractual relationship with a client from the region may have a low risk of money laundering. For example, a client that trades goods with a client from a country in the region may be low-risk because there is an economic justification for such a relationship.

Or, for example, a low-risk party may be one that is registered for the trade of goods and where, upon further monitoring of the business, it is concluded that all transactions with suppliers and customers are related to the business it performs and are not registered at destinations that would indicate a possible increased risk.

II Client risk

The obliged entity independently determines the approach to the client's risk, based on generally accepted principles and own experiences. Activities carried out by the following clients may indicate a higher risk:

1) clients that conduct business activities or transactions under unusual circumstances, which means:

- the client assigns receivables for goods that are not typical of its business (e.g. production of medicines, sales of frozen fruit);
- the client assigns claims from the debtor that are not in accordance with the economic feasibility and/or the assignor and the debtor or with the activity;
- the client offers guarantees from third clients without any business logic or from persons with a bad reputation;
- economic dependence or affiliation of the client and management factors;
- knowledge of how factors work;
- frequent and unexpected establishment of business relationships with multiple obliged entities of the same activities, without economic justification.

2) clients where:

- due to their structure, legal form or complex and unclear relationships, it is difficult to determine the identity of their beneficial owners or the persons who manage them, such as offshore legal entities with an unclear ownership structure that are not established by companies from a country that applies standards in the field of preventing money laundering and terrorist financing that are at the level of the standards prescribed by the Law;
- fiduciary or other similar company under foreign law with unknown or hidden owners or management (this is a company under foreign law that offers to perform agency services for a third party, i.e. a company established by a contract concluded between the founder and the manager, which manages the founder's assets, for the benefit of certain users or beneficiaries, or for other specific purposes);
- complex status structure or complex chain of ownership (complex ownership structure or complex chain of ownership that makes it difficult or impossible to determine the beneficial owner of the client, i.e. the person who indirectly provides the assets, on the basis of which they have the possibility of supervision, which may direct or otherwise significantly influence the decisions of the client's management or executive board when deciding on financing and operations);

3) foreign arms dealers and arms manufacturers;

4) non-residents and foreigners;

5) clients who are represented by professionals (lawyers, accountants or other professionals), especially when the obliged entity is in contact only with these porfessionals;

6) companies with a disproportionately small number of employees in relation to the volume of work they perform, which do not have their own infrastructure and business premises, where there is an unclear ownership structure etc.;

7) persons with a bad reputation, either public or from previous experiences, selling other products, etc .;

8) clients report claims that are not in accordance with the economic possibilities and activities of the creditor;

9) officials, in accordance with the Law;

10) a client that is a foreign legal person, which does not carry out or is prohibited from carrying out trade, production or other activities in the country in which it is registered (a legal person headquartered in a country known as an offshore financial center);

11) clients suspected of not acting on their own behalf, i.e. carrying out instructions from a third party;

12) establishment of companies or foreign legal entities as single-member limited liability companies, with a minimum share capital, registered for the activities of non-specialized wholesale trade, consulting, marketing and IT services and activities related to construction, including the drafting of articles of association and their notarization;

13) change in the ownership and management structure of companies or foreign legal entities established as single-member limited liability companies, with minimal share capital, fewer than three employees and disproportionately high revenues generated in a short period of time, including the preparation of acts on status changes and their notarization;

14) disproportionate prices of goods - where the purchase or sale price of dual-use goods or military goods is significantly higher or lower than the market value, potentially indicating attempts to justify the transaction under suspicious circumstances (e.g. motivation of a foreign partner for long-term business) ;

15) unusual trade routes or excessive transport costs - when export declarations include unusual trade routes that significantly increase transport costs, such as the route of goods through Serbia, rather than directly to the final destination, which may suggest an intention to conceal the true origin or destination of the goods ;

16) and shipments to high-risk jurisdictions that include countries or entities designated for low levels of transparency, especially when the purpose, storage and end-use of large quantities of military equipment are unclear or contrary to the needs of the destination country.

17) end-user or foreign partner with a suspicious background - cases in which due diligence reveals that the end-user or foreign partner has a history of criminal convictions related to illegal trade practices or is subject to trade prohibitions ;

18) The purchasing of old or surplus military equipment by wealthy nations - export licensing requirements that involve wealthy nations purchasing obsolete military equipment, where there is no obvious strategic reason for purchasing older items over more modern alternatives, leading to questions about the intended use or destination of these goods.

III Transaction risk

Transaction risk includes the following transactions:

1) transactions that significantly deviate from the client's standard behavior;

2) transactions that do not have economic justification;

3) transactions that are conducted in a manner that avoids standard and customary control methods;

4) transactions in which the client refuses to provide all documentation, as well as transactions in which the documentation does not correspond to the manner of conducting the transaction itself ;

5) transactions where there are frequent changes to credit notes, discrepancies or contradictions between the invoice and the description;

6) transactions that were intended for persons or entities against whom United Nations or Council of Europe measures are in force, as well as transactions that the client would carry out on behalf of and for the account of a person or entity against whom United Nations or Council of Europe measures are in force;

7) business relationships or transactions arising from re-export transactions;

8) frequent or large-scale transactions related to the payment of winnings from online games of chance;

9) crowdfunding;

10) business relationships or transactions related to digital assets that include large-value transactions in stable digital assets, transactions that are carried out outside of a payment account – such as P2P transactions, as well as transactions where it is difficult or impossible to determine the origin of funds;

11) business relationships or transactions involving digital asset service providers in jurisdictions that do not apply international standards for the prevention of money laundering and terrorist financing in the field of digital assets;

12) business relations or transactions with a person involved in the trade of weapons, military equipment or dual-use items;

13) business relationships or transactions with a person involved in the trade of gold and works of art;

14) transactions related to the legalization of constructed real estate;

15) unusual one-off transactions that are not consistent with the typical financial behavior of the client, especially large or complex transactions that are not consistent with the normal business activities of the individual or entity, may signal an attempt to exploit the financial system of Serbia

for the purposes of PF (this is particularly relevant for transactions involving foreign persons who have no clear ties to Serbia);

16) The use of shell companies or complex corporate structures - more often shell companies, especially those with unclear ownership structures or newly formed entities, in financial transactions may indicate efforts to conceal the true nature of the transaction. This is a red flag when such companies are used in one-off deals or transactions involving dual-use goods or other sensitive items ;

17) Transactions involving high-risk jurisdictions - financial transactions involving countries known to be involved in proliferation activities are significant red flags. This includes transfers of funds to or from these jurisdictions, particularly when the purpose of the transaction is unclear or does not match the profile of the clients involved ;

18) the increased use of non-resident individuals or entities in financial transactions within Serbia, especially those with no obvious business or personal ties to the state, could suggest an attempt to exploit the Serbian financial system for PF;

19) and sudden changes in business activity - a domestic company or financial institution suddenly engaging in activities involving high-value goods, dual-use technologies, or significant cross-border transactions, especially when there is no prior history of such activity, may indicate an attempt to use the company or institution as a conduit for PF.

IV Service risk

Service risk refers to the following risky services:

1) services that are new to the market, i.e. not previously offered in the financial and non-financial sectors, and must therefore be specifically monitored to determine the actual level of risk;

2) providing those services for which the employees of the obliged entity, based on their experience, assess that carry a high degree of risk;

3) All negotiable instruments made out to bearer, but also negotiable instruments issued in favor of a fictitious payee, endorsed without restriction or in other forms that allow transfer of title upon delivery, and all other incomplete instruments that are signed but without the payee's name listed, may be considered as services that pose a high risk for money laundering and terrorist financing.

In addition to the previously mentioned criteria, when determining the level of risk of an individual party, business relationship, service or transaction, the obliged entity should also include other types of risk or other criteria, such as:

- the size, structure and activity of the client, including the scope, structure and complexity of the business carried out by the client;
- status and ownership structure of the client;
- the purpose of entering into a business relationship, providing a service or executing a transaction;
- knowledge of the services and its experience, i.e. knowledge in that area;

- other information that indicates that a customer, business relationship, service or transaction may pose a higher risk.

Transitional and final provisions

On the date of entry into force of these Guidelines, the "Guidelines for assessing the risk of money laundering and terrorist financing for entrepreneurs and legal entities engaged in the provision of accounting services and factoring companies" of 22 March 2022 shall cease to be valid .

These Guidelines are published on the website of the APML. Obliged entitiess are obliged to bring their internal acts into line with these Guidelines within 30 days from the date of publication on the website of the APML

Belgrade, 9 May 2025

Director

Željko Radovanović