Pursuant to Article 114 of the Law on Prevention of Money Laundering and Terrorism Financing (Official Gazette of RS, No 113/2017) within the scope of its authority under Article 104 of this Law, the Securities Commission (at its 74th session of the IX term of office, on 8 November 2018) hereby adopts

GUIDELINES

for assessing money laundering and terrorism financing risks and application of the Law on Prevention of Money Laundering and Terrorism Financing for entities supervised by the Securities Commission

(aligned with the National Assessment of Money Laundering Risks and Terrorism Financing, from 2018)

OBJECTIVES OF THE GUIDELINES

The Securities Commission (hereinafter: the Commission) within the scope of its authority under the Law on Prevention of Money Laundering and Terrorism Financing (hereinafter: the Law) to independently adopt guidelines for the implementation of the provisions of the Law. The Guidelines for Money Laundering and Terrorism Financing Risk Assessment and Application of the Law on Prevention of Money Laundering and Terrorism Financing for Entities supervised by the Securities Commission (hereinafter: the Guidelines): for the uniform application of provisions of the Law by:

1. Investment fund management companies licensed to perform the investment fund management activities, in accordance with the law governing operation of investment fund management companies,

2. Broker-dealer companies whose regular occupation or business is the provision of one or more investment services to third parties, or the performance of one or more investment activities on a professional basis, in accordance with the law governing capital market,

3. Authorized banks, which are organizational units of credit institutions and whose regular occupation or business is the provision of one or more investment services to third parties or performance of one or more investment activities on a professional basis, involving one or more financial instruments, in accordance with the law governing capital market,

4. Custody banks, authorized to carry out custody activities – set forth by the law governing operation of investment funds,

(Hereinafter referred to as: reporting entities).

The Securities Commission supervises implementation of the Law by the reporting entities, in accordance with the law governing capital market, the law regulating takeovers of joint stock companies and the law governing operations of investment funds.

With the adoption of the 2009 Law on Prevention of Money Laundering and Terrorism Financing, the Republic of Serbia achieved compliance with the international standards in the field of anti-money laundering and terrorism financing adopted by the Financial Action Task Force (FATF) and the relevant European Union *acquis*. The risk-based approach entailing analysis and assessment of risk from money laundering and terrorism financing, the reporting entities perform for each client, was introduced. The Law on Prevention of Money Laundering and Terrorism Financing from 2017 widens the scope of risk assessment to the level of respective reporting entities.

The state was required to formulate the national money laundering and terrorism financing risk assessment, and to define measures and activities that need to be in place in order to mitigate the recognized risks. The national assessment results provide necessary information to reporting entities and serve as a starting and mandatory point in risk assessments performed by respective reporting entities within their institutions. Reporting entities need to comprehend and apply the risks assessed at the state level.

The Guidelines do not entail the correct order of steps for the reporting entities in application of their internal risk assessments, but provide for better understanding of risks at the level of reporting entities and assist how certain activities are to be executed.

All who participate in the money laundering and terrorism financing risk assessment can obtain additional information in other materials, guidelines, publications etc. The FATF website contains various sectoral guidelines for risk based approach.

The goal of the Guidelines is to direct reporting entities how to conduct the general money-laundering and terrorism-financing risk assessment in their operations, and how to

conduct risk assessment and analysis in individual cases, where business relations are established (with clients, partners, parties to a contract etc.). Any institution, regardless of size and complexity of organization, must have an adequate money-laundering and terrorism-financing risk management system in place. The system must provide that the risks are being comprehensively identified, assessed, monitored, mitigated and managed. Reporting entities can apply the measures to different extents, depending on the type and level of risk involved and the different risk factors.

The reporting entities are expected to establish whether a criminal offense of money laundering or terrorism financing has been committed. The principal task of a reporting entity is to have at disposal all the necessary information concerning knowing the customer and monitoring of their business transactions, to assess whether certain types of behavior can be linked to a criminal offense and to what extent, and to take all the appropriate measures and report suspicious activities in accordance with the Law. The Administration for Prevention of Money Laundering and investigative authorities conduct further procedures in the case, in order to establish whether there are elements of criminal offense.

The Guidelines contain examples characteristic of money laundering and terrorism financing risks for reporting entities supervised by the Commission.

WHAT IS "MONEY LAUNDERING"?

The Law defines money laundering as:

1) conversion or transfer of property acquired through the commission of a criminal offense;

2) concealment or misrepresentation of the true nature, source, location, movement, disposition, ownership of or rights with respect to the property acquired through the commission of a criminal offense;

3) acquisition, possession, or use of property acquired through the commission of a criminal offense.

Money laundering includes a number of activities undertaken in order to conceal the origin of proprietary gain acquired through the commission of a criminal offense. The money laundering process might involve a series of transactions carried out both in the gray economy and in the formal (legal) sector. In the gray sector, the assets acquired through commission of criminal offenses enter the system and exit as legitimate goods and services.

Anyone who provides services or deliver products may be used as an instrument in money laundering. Money can be laundered through financial sector operations, and through operations outside the financial sector. When property is acquired through the

commission of a criminal offense, the perpetrator seeks ways to use the money in ways which do not attract attention of competent authorities. Therefore, the perpetrator carries out a set of transactions intended to represent the money as legitimate.

Money laundering occurs in three phases:

1. First phase: "Placement" entails severing of the direct link between the money and the illegal activity in which the money has been obtained. This is the stage of money laundering at which illegal money first enters the financial system. The money is paid into banking accounts, most often under a pretense of legal activity for which cash payment is entailed (for example, foundation of a fictitious company with no business activities, which serves solely as an instrument for placing illegal money or fragmenting large sums of money then placed into accounts in non-suspicious amounts for which reporting is not required).

2. Second phase: Layering. After the money has entered the legal financial system, it is transferred from the account where it has been deposited to other accounts of companies with an aim to represent a fictitious business activity or to perform a legal transaction (trade or service) with legitimate companies. Such transactions have no economic or business purpose. The main goal of the transactions is to cover the connection between the money and the criminal activity in which the assets were acquired, to conceal the trace of money and hinder all those trying to establish the origin of assets.

3. Third phase: Integration, in which illegal proceeds show as money originating from a legitimate activity (for example, a common integration method of illegal money into legal financial flows is property buying or purchase of controlling blocks of shares of shareholding companies, concentrating illegal capital in huge amounts, the aim of money launderers). Integration is concentrated on market values that is, what can be bought and sold (e.g., purchased property is rented and the rent money does not represent suspicious proceeds). Money is often invested in companies in distress, which afterwards continue to operate with success and the results of their operations are legitimate proceeds). When the money enters this phase it is very difficult to discover its illegitimate origin.

The listed stages of money laundering need not be in the presented order (illegal funds can be directly invested in luxurious goods or immovable property). In some cases of criminal offenses, such as misappropriation of funds and fraud in the area of investments, the money is already in the financial system and there is no need for it to be integrated into the system). In addition, before the illegal money is introduced into the financial system, it is

often moved either physically or via post, or courier services, or through the money transfer systems.

WHAT IS TERRORISM FINANCING?

In the context of the law, terrorism financing means the providing or collecting of property, or an attempt to do so, with the intention of using it, or in the knowledge that it may be used, in full or in part:

1) in order to carry out a terrorist act;

2) by terrorists;

3) by terrorist organizations.

Terrorism financing means aiding and abetting in the provision or collection of property, regardless of whether a terrorist act was committed or whether property was used for the commission of the terrorist act.

Terrorism financing is a special form of financial crime. The main goal of individuals and organizations involved in terrorism financing need not necessarily be concealment of source of financial assets, but it is primarily the intention to hide the nature of activities for which the assets are intended. Terrorists use an array of different methods to move money to satisfy the needs of their organizations and activities, including financial sector activities, cash transfers, trade, donations, charity organizations and formal and informal money remittance systems.

Terrorism financing proceeds might come from legal sources, such as donations, profit generated from legal businesses, charity organizations and from illegal sources alike, such as drug smuggling, smuggling of weapons, gold and diamonds, i.e. misappropriation of funds, kidnapping, extortion etc.

There are four stages in terrorism financing:

1. Raising funds from legitimate operations and from criminal activities

2. Holding raised funds

3. Transfer of funds to terrorist

4. Use of funds.

The first phase includes raising funds from legitimate sources, connected with terrorism organizations or terrorists, or from persons linked to criminal activities such as drug trafficking, extortion, embezzlement etc. Individual donations represent a significant source of funds, by persons who support goals of terrorist organizations, or funds, which collect money and direct it to terrorist organizations.

In the second phase, the funds are kept in accounts of persons or intermediaries – persons linked with terrorist organizations.

The third phase involves transfer of funds to cells of terrorist organizations, i.e. individuals who utilize the funds to pursue their terrorism objectives. The most employed avenues to move funds are the money remittance systems and the banking system. Although, there is a large number of cases of informal ways of moving funds.

The use of funds becomes obvious when used for terrorism – purchase of explosives, financing terrorist training camps, promotion, political support, sheltering purposes etc.

Money laundering and terrorism financing are global issues which might have an adverse effect on economic, political, security and social structure of a state. The consequences of money laundering and terrorism financing are undermined stability, transparency and efficiency of state financial systems. They cause economic disruptions and instability, damage reputation and imperil national security.

Money laundering and terrorism financing risks also occur due to failures in application of legislation, where a reporting entity may be exposed to risk from compromising own integrity and reputation following a sanction by a supervisory authority.

An efficient system combating money laundering and terrorism financing entails analysis of both risks.

WHAT IS A SUSPICIOUS TRANSACTION?

A suspicious transactions may be a transaction for which a reporting entity and/or a competent authority estimate that there are reasons for suspicion of money laundering or

terrorism financing regarding a person or transaction, i.e. that a transaction includes illicit money.

Suspicious transactions are also those which according to their nature, scale, complexity or relatedness are unusual, i.e. which have no apparent economic or visible lawful purpose, or transactions that are inconsistent, disproportionate to the usual or expected business operations of a customer and other circumstances pertaining to the status or other characteristics of a customer. Certain transactions but also business relations of a customer can be regarded as suspicious.

Determining how suspicious a customer, transaction or a business relation is, is founded on criteria set in the List of Indicators developed for the recognition of persons and transactions with respect to which there are reasons for suspicion of money laundering or terrorism financing. The Lists of Indicators represent a starting point for employees/authorized persons when recognizing suspicious circumstances with respect to a customer, transactions of the customer or business relations it concludes. Therefore, all employees of a reporting entity must be familiar with the indicators in order to use them in their work. When determining a suspicious transaction, an authorized person shall provide all technical assistance to employees.

CORE PRINCIPLES IN COMBATING MONEY LAUNDERING AND TERRORISM FINANCING

When performing their registered activities, obligors are required to act in conformity with the Law and stipulated obligations governing the detection and prevention of money laundering and terrorism financing and to ensure adherence to statutory measures and activities of obligors at all levels, so that entire business operations of an obligor are carried out in accordance with the Law.

Actions and measures for the prevention and detection of money laundering and terrorism financing should be taken before, in the course of, and following the execution of a transaction or establishment of a business relationship and they include:

1) customer due diligence;

2) sending information, data, and documentation to the Administration for Prevention of Money Laundering (APML);

3) designating persons responsible for complying with the obligations laid down in the Law (compliance officers) and their deputies, and providing conditions for their work;

4) regular professional education, training and capacity building of employees;

5) providing for regular internal control of complying with the obligations laid down in the Law, and internal audit if in accordance with the scope and nature of business operations of the reporting entity;

6) developing a list of indicators for identifying persons and transactions with respect to which there are reasons to suspect money laundering or terrorism financing;

7) record keeping, protection and retention of data from such records;

8) implementing measures laid down in the Law by reporting entity branches and majority-owned subsidiaries located in foreign countries;

9) implementing other actions and measures based on the Law.

A reporting entity is required to set down appropriate internal enactments encompassing all the required actions and measures defined in the Law, for effective management of money laundering and terrorism financing risks. Internal enactments must be commensurate to the nature and size of the reporting entity and approved by the top management. (Article 5 of the Law) In addition to all the listed actions and measures for prevention and detection of money laundering and terrorism financing, reporting entities are required to develop risk analysis of money laundering and terrorism financing (Article 6 of the Law).

RISK ASSESSMENTS AND ANALYSIS

In order to prevent exposure to adverse effects of money laundering and terrorism financing, a reporting entity must comprise and regularly update an analysis of money laundering and terrorism financing risks, in accordance with the law (hereinafter: risk analysis).

The risk analysis determines the level of exposure (risk assessment) for each group and type of customer, business relation, service the obligor provides within its activity or transaction to money laundering and terrorism financing risk.

Risk analysis must be commensurate to the nature and scope of business and the size of the reporting entity, it must consider the main types of risk (customer, geographic, transaction and service risk) and other types of risk the reporting entity has identified relative to the specific character of their business.

Risk analysis comprises:

1) risk analysis relative to overall business of a reporting entity;

2) risk analysis for each group or type of customer i.e. business relationship, or service reporting entity provides within their business activity, or transaction.

Pursuant to their risk analysis, a reporting entity classifies customers in one of the following risk categories:

1) low money-laundering and terrorism-financing risk and applies at least simplified customer due diligence;

2) moderate money-laundering and terrorism-financing risk and applies at least general customer due diligence;

3) high money-laundering and terrorism-financing risk and applies enhanced customer due diligence.

In addition to these risk categories, a reporting entity may in its internal enactments envision additional risk categories and define adequate actions and measures for such risk categories.

A reporting entity must establish internal procedures - money laundering and terrorism financing risk analysis, especially in the part of:

- determining risk relative to overall business of the reporting entity;
- determining the identity of a customer, verification of identity based on documents, data or information obtained from reliable and credible sources;
- determining identity of beneficial owners of the customer and verification of their identity;
- obtaining information on the purpose of the business relation or a transaction; obtain and assess the credibility of information on the origin of property which is or which will be the subject matter of the business relationship or transaction, in line with the risk assessment;
- regular monitoring of customer's business transactions and checking the consistency of the customer’s activities with the nature of business relationship and the usual scope and type of the customer’s business transactions.

It is of special importance that all employees be acquainted with the procedures, act according to the procedures and use them in their work.

The internal procedures of reporting entities include: Regular training, on-the-job/professional development and capacity building of employees, internal control mechanisms, detection and notification procedures on suspicious transactions, responsibility of employees for the implementation of measures for detection and prevention of money laundering and terrorism financing.

Planning and organization of risk analysis process is important for the end result of risk assessment. The essence of an efficient and quality process of devising and updating risk assessment is to first determine parts of the system which might have essential information within the reporting entity, able to identify vulnerabilities in the system and to decrease risk (for example, a broker in a broker-dealer company or an internal controller will contribute more to the risk analysis process than a person who has no direct contact with clients). In addition to the parts of the system within a reporting entity which might have essential information for risk assessment, a reporting entity must not disregard the so called external sources of information.

(*For example, results of the National Risk Assessment and vulnerabilities of the financial system from money laundering and terrorism financing, research by a supervisory authority, information from the control, notifications, amendments to the legal framework might indirectly affect application of anti-money-laundering and terrorism-financing regulations. Further, this includes information from prosecution, charges brought, models of behavior identified in charges for money laundering, reporting entities exposed to activities of criminal groups and attempts at presenting illegal money as clean, information from the Administration for Prevention of Money Laundering, number of suspicious transactions, rationale for reporting a suspicious transaction, strategic analyses, typologies, information contained in annual statements etc. Also, a very important source of information is feedback received by reporting entities on reported suspicious transactions. Moreover, in addition to information which can be obtained in the country, international research is of importance as well, by Council of Europe, OSCE, FATF and other)*.

Employees working for a reporting entity must have a clear picture of how the reporting entity assessed institution risks, how the state risks have been implemented in the process and how it provided a clear overview of measures it intends to implement on the basis of results obtained.

The purpose of risk analysis

Risk analysis preparation is a precondition for implementation of customer due diligence. Depending on the classification of customer, business relation or transaction into a risk category, a reporting entity shall carry out the type of risk-based analysis in accordance with the Law (customer due diligence, enhanced due diligence and simplified due diligence for the low-risk group).

When devising their risk analysis a reporting entity must take into account the main types of risk (customer, geographic, transaction and service risk) and other types of risk the reporting entity has identified relative to the specific character of their business.

Risk assessment – definition

Risk depends on three factors: threat, vulnerability and consequence.

Risk assessment is making a judgment on threats, vulnerabilities and consequences.

Threat includes persons i.e. activities with a potential to inflict harm (for example in a reporting entity clients identified or for whom there is suspicion that they are linked to illegal activities, detected fraud, forged documents etc. might harm to the institution, business operation, its reputation).

The term vulnerability in the context used in risk assessment encompasses all the activities which might be used in cases of a threat. The focus is on the activities which represent weaknesses in the system of money laundering and terrorism financing and the control system. When it comes to a reporting entity, vulnerability is all what makes an institution particularly exposed to money laundering or terrorism financing (*for example, a service offered by the reporting entity, assessed as bearing high risk at the level of the state, insufficient knowledge of the regulations governing this area, inadequate application of regulations and similar)*.

Consequence means damage which money laundering or terrorism financing might cause and encompasses effects of illegal or terrorist activities on the financial system and institutions, and furthermore on society and economy. Consequences can be short-term and long-term and affect reputation and appeal of financial sector, i.e. non-financial sector of a state (for example: A consequence might be measured by the amount of sanction imposed to a broker-dealer company for failing to adequately react to risks, or by undermined reputation of a reporting entity for whom it is established that through inadequate risk analysis and mitigation measures aided money laundering or terrorism financing).

Risk Assessment Stages

The risk assessment procedure can be divided into a set of activities, but the main stages of the process are:

1. risk identification,

2. analysis,

3. evaluation and risk management.

A reporting entity must take into account conclusions reached in the National risk assessment and how the overall environment and risk activities affect their business. For example, if the National Risk Assessment entails low risk for capital market institutions, and in total for the whole country middle level of risk from money laundering and terrorism financing is established, then a reporting entity must analyze factors which affected the results of the national risk assessment. The entity shall consider these factors when analyzing risk of their operations and risk of their clients).

Republic of Serbia National Risk Assessment

The comprehensive National money laundering risk assessment and the National terrorism financing risk assessment, adopted by the Government of the Republic of Serbia in May 2018, was conducted according to the World Bank methodology in four thematic areas:

1. money laundering threat assessment;

2. vulnerabilities from money laundering at the national level;

3. sectoral vulnerability;

4. terrorism financing risk assessment.

Money laundering risk assessment is a result of the assessment of money laundering threats (based, inter alia, on the predicate crimes) and the national vulnerability from money laundering.

Based on the analysis of the predicate crimes, overview of threats per sectors and the cross-border threats, the overall money laundering threat assessment is "**medium"** with a "**no change tendency**".

The national vulnerability from money laundering has been assessed as **medium**, based on the analysis of the state's ability to ward off money laundering and on the analysis of the sectoral vulnerability.

The analysis conducted with the purpose to achieve this aim for the Republic of Serbia demonstrated that **the overall money laundering risk is medium**.

Money laundering threat assessment

Predicate crimes which pose a high level of money laundering threat are: tax crimes, abuse of office by the responsible officer, abuse of office by an official, unauthorized production and trafficking of narcotics.

Predicate crimes of a medium threat level include: illegal crossing of state border and human trafficking, aggravated larceny, robbery, fraud, extortion, illegal trade, corruption crimes (giving and accepting bribes and influence peddling). These crimes are predominantly committed for purposes of obtaining proprietary gain which is then laundered. Procedures were initiated and led for the criminal offense of money laundering and it confirms the money laundering threat potential. Other criminal offenses are criminal offenses bearing **low levels of money laundering threats**.

High technology crimes pose **a growing threat** in terms of money laundering, especially business email scams (the BEC – business e-mail compromise). It targets companies with significant financial resources. Therefore, these high technology crimes generate high amounts of illegal proceeds. Cash flows are difficult to detect, especially if converted into cryptocurrencies, and their prosecution is more difficult as perpetrators are unknown.

The most of the predicate criminal offenses are committed in the national jurisdiction, therefore the threat is high.

The sectors most exposed to money laundering threats are the real estate sector (investments in residential and business buildings, purchases of properties), games of chance providers (with high turnover volumes of money, mostly cash) and the banking sector. The banking sector is still one of the most exposed to money laundering threats, for its size and importance within the financial market and the number of services and products. They are followed by the currency exchange offices. Serbia still has large volumes of payment executed in cash. As a consequence, foreign currencies are often converted into dinars and vice versa. Then, casinos are the next in line (active cash sector in which payments are conducted in cash) followed by the accountants (companies which took part in money laundering used the services of accounting agencies to cover the criminal activities by a pretense of legal business activities).

Based on the analyses conducted, the organizational forms of companies in terms of money laundering threats, applying the criteria of size and number of money laundering cases where companies were included in money laundering - limited liability companies were classified as high level treat, entrepreneurs as medium level threat, joint stock companies as bearing medium level threat and other forms of organization (limited partnerships and general partnerships) as posing a low level of threat.

When conducting a risk assessment, reporting entities supervised by the Securities Commission, must take into account the sectoral risk assessment, in the procedure assessing the risk in terms of the overall business of the reporting entity and in analyzing the risks for each group or type of a customer, business relation, service offered by the reporting entity and transaction.

Here follows an overview of threats per sectors.

Table 1. Sectoral threats

Sector	Degree of threat
real estate	high
games of chance	high
banks	high
exchange offices	medium high
casinos	medium high
accountants	medium high
attorneys/lawyers	medium
payment institutions	medium
capital market	medium low
auditors	medium low
leasing	medium low
notaries	low
factoring	low
insurance companies	low
pension funds	low

Vulnerability assessment of the system from money laundering

Based on the data and information collected, in view of the money laundering threats, the national combating ability has been assessed as "medium".

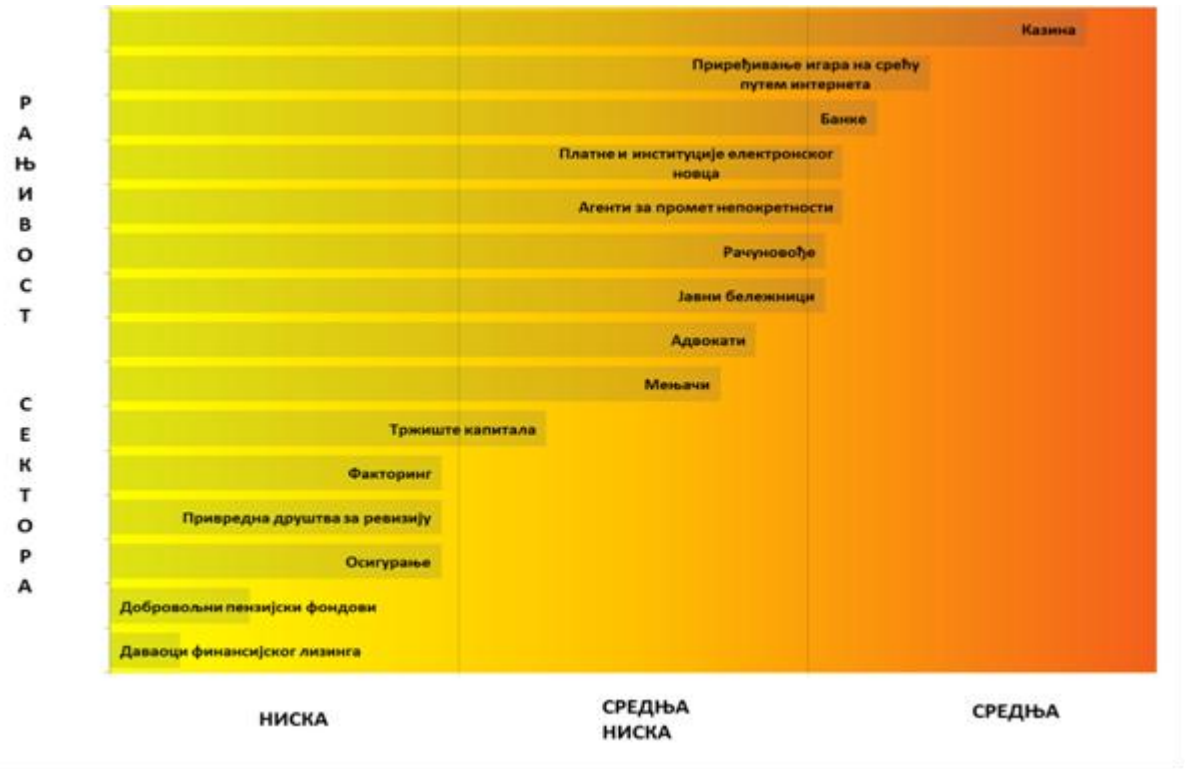
Sectoral vulnerability - In addition to the money laundering national combating ability, the national vulnerability is affected by vulnerability of some of the sectors which could be used for money laundering purposes. To that end, great attention in devising the National Risk Assessment was dedicated to data processing and analysis of the Republic of Serbia financial and non-financial systems.

Vulnerability assessment of the securities sector

The vulnerability assessment of the securities sector (capital market) in the Republic of Serbia is medium-low, which means that the risk of money laundering and terrorist financing in this sector exists, but at a lower level. Such an assessment was made based on the established circumstances relating to the underdeveloped and shallow capital market, a low share of the capital market in the composition of the financial system of the Republic of Serbia, the illiquid market, a large proportion of inactive customers, the fact that reporting entities do not operate with cash transactions (all payments are made through bank accounts), strict regulations in this area, risk-based supervision, and the consistent application of adopted regulations, both by reporting entities and by the supervisory body, the Securities Commission.

Here follows an overview of vulnerabilities per sectors.

Table: an overview of vulnerabilities per sectors



Terrorism financing risk assessment at the national level was carried out by consideration of terrorism threats, effects on the terrorism financing threat and threat from terrorism financing and vulnerability. The assessment also analyzed the NPO sector from the aspect of terrorism financing vulnerability.

The following criteria were assessed: “Terrorism Threat", "Terrorist Financing Threat" and "Terrorist Financing Vulnerability" on the basis of the overall parameters and statistical data. The Working Group has made an assessment that the level of the "Terrorist Financing Risk" in the Republic of Serbia is "**medium**".

The document Money Laundering Risk Assessment and Terrorism Financing Risk Assessment of the Republic of Serbia was published on the website of the Administration for the Prevention of Money Laundering. In addition to threats and vulnerabilities information determined in the national risk assessment, all the other analyses of threats are of use – typologies and trends recognized in reports of the Administration for Prevention of Money Laundering, supervisory authorities, international institutions and similar.

1. RISK IDENTIFICATION

Identification starts with identifying risk. It would be useful for reporting entities to devise a list of factors to be used in recognizing threats and deficiencies in a reporting entity in money laundering i.e. terrorism financing. The list should contain all the factors recognized as risk by the state, which are characteristic of a reporting entity, typologies recognized in cases of money laundering and terrorism financing, trends and circumstances established by the supervisory authority as not comprehended sufficiently when it comes to application of the Law. (*For example, if the state recognizes companies from a region as carrying risk, it is important whether a reporting entity has recognized transactions with these companies, as carrying risk, how the entity rated the companies in the past, potential undetected abuses by these clients, the reasons why the transactions by these clients were not recognized as risky in terms of money laundering. Moreover, whether the reporting entity has recognized situations in which a client has come under investigation at a later point, but at the moment of transaction was not recognized as risky, and whether a reporting entity could have had the information or not*).

Having compiled a comprehensive and wide list, a reporting entity can discern which of the factors is not sufficiently significant for the reporting entity or maybe the situation may be that the reporting entity is not offering a product recognized at the level of the state as risky, or certain models of behavior are not characteristic of the reporting entity. This means that certain points can be eliminated from the list, but if certain behavior models or circumstances occurred in the past and proved risky, they should be on the list and analyzed separately.

At this stage, it is not possible to say that a factor is more or less risky. However, we can talk about whether a factor is relevant enough to assess money laundering or terrorism financing risk. (*For example, approaches can differ depending on a reporting entity. Thus, a reporting entity may decide to use as a starting point behavior models, indicators, trends and estimates made at the state level and then to analyze to what extent the estimates would be relevant to the reporting entity. Furthermore, another reporting entity might decide to start with risk bearing services, transactions, and to further work on the first estimates, including certain recognized typologies, for example for certain services or executed transaction, but to certainly take into account results of the national risk assessment*).

There is no universal model for devising the risk assessment, only guidance, ideas, proposals, national and international practice. It is on the reporting entity to estimate which methodology suits their business. (*For example, factors of importance to be placed on the list: type of recognized criminal activities in the previous period, whether the criminal activities were suspected or confirmed, whether clients were connected with illegal activities (media, conversations and similar), transfers to high-risk countries, transfers from high-risk*

countries, amounts of cash transactions, amounts of suspicious reports, legal framework, harmonization of legal provisions, number of clients, companies' share, share of natural persons, results of supervisory proceedings, supervision findings for certain sectors, number of suspicious reports, feedback on suspicious reports, system in which it operates, obtaining a license/authorization, procedures for commencing business operations, communications with state authorities, effect of procedures of the group on the reporting entity, all products from the national risk assessment, all services from the national risk assessment, trends recognized in the national risk assessment, methods for laundering money i.e. financing terrorism recognized in the national risk assessment, types of companies etc.)

A reporting entity may assess money laundering risk separately from the terrorism financing risk. Reporting entities whose business is carried out mainly in cash must be separately monitored for higher terrorism financing risk. To that end, special attention needs to be placed on operations of non-profit organizations as they bear high potential for abuse in terms of terrorism financing. When it comes to terrorism financing, geographic/country risk is intensive in regions where, based on information from relevant international organizations such as the United Nations, there are terrorist activities.

RISK CATEGORIES

Recognizing a risk category – customer risk, transaction risk, service risk, risk of different types of business operation, geographic/country risk, is a first step for risk analysis both for the reporting entity and the customer. Please note that risk categories may differ depending on the specific characteristics of business of a reporting entity and that each reporting entity is to take into account categories of risk relevant to their scope of work.

Country Risk

Country risk (or sometimes referred to as geographic risk) means the estimate of ML/TF risk exposure depending on the area/country of origin of the customer, country of origin of the majority founder i.e. the owner of customer or a person that in any other manner exercises controlling influence over the management of customer and their operations, as well as the country of origin of the person performing transactions with the customer.

Factors that may result in determination that a country poses a higher ML/FT risk include:

1) Countries subject to sanctions, embargoes or similar measures issued by the United Nations, Council of Europe or other international organizations;

2) Countries identified by credible institutions (Financial Action Task Force - FATF, Council of Europe, IMF, World Bank and other) as lacking application of appropriate AML/CFT measures. Here especially noting the process of the FATF International Co-operation Review Group (ICRG). After each of the meetings FATF issues a list of countries which according to the ICRG do not possess an adequate system for combating money laundering and terrorism financing.

3) Countries identified by credible institutions (FATF, UN and others) as providing funding for or support to terrorist activities or organizations;

4) Countries identified by credible institutions (e.g. World Bank, IMF) as high-risk jurisdictions, with high risk of corruption and criminal.

5) off-shore legal persons, in accordance with the Law.

(*For example, assessment and appraisal of risk depends on the location of a reporting entity, their organizational units, which means it will differ with reporting entities located in cities and towns. Customers from the region might entail less risk than the customers outside of the region or the country with which we do not have any business relations at all. Transactions executed on off-shore destinations also entail increased ML/FT risk.)*

Based on the authority granted by the Law, the Minister of Finance adopts a list of countries that apply AML/CTF international standards at least at the level of the European Union (the White List), and the list of countries that do not apply any standards in the area (the Black List).

Reporting entities use the lists to assess customer risk, meaning that the customer from a country on the Black List will bear higher risk in relation to the customer originating from the country on the White List. Categorization into high risk will require application of enhanced customer due diligence actions and measures.

Customers, parties to a contract with persons from off-shore countries and doing business with persons from off-shore countries also bear higher ML/TF risk. A reporting entity must establish a procedure determining whether a customer or a legal person in the ownership of the customer is an off-shore legal person, in accordance with the Law. In this regard, a reporting entity may use lists issued by the IMF, World Bank or a list of countries from the Rulebook governing a list of jurisdictions with a preferential tax system (Official Gazette of RS, No 122/12), in order to establish whether a person is off-shore (for example, for a broker-dealer company a high risk customer will be the customer performing agreed block transactions in shares, especially when the buyers are unknown, newly-formed companies from off-shore destinations. Moreover, higher ML/TF risk is understood when a customer originates from a country which based on the information from relevant international institutions and the Administration for the prevention of money laundering fails to apply the AML/TF standards or trades in such jurisdictions. Another example of high

risk is trading in securities on behalf of legal persons from off-shore destinations using custody banks in activities of managing trading accounts or settling transactions in order to conceal their identities).

Customer risk

A reporting entity determines, on their own, customer-risk-based approach, following the generally accepted principles and own experience. Customer risk entails assessment whether a customer is connected with higher risk from money laundering and terrorism financing.

The following customer activities may indicate higher risk:

1) When establishing a business relationship, the customer fails to appear in person and insist on indirect contact;

2) A customer builds their business relations or performs transactions in unusual circumstances, such as:

- significant and unexplained distances to locations to conduct transaction or establish a business relationship,

- frequent and unexplained establishment of business relations of similar kind with multiple reporting entities without an economic purpose, such as opening accounts with multiple reporting entities, conclusion of several contracts on the provision of services over a short period of time and similar,

- termination of membership immediately after the conclusion of a fund membership contract;

- a request to transfer funds accumulated on the individual account of a fund member to a current account of a third person, or to an account in a country that does not apply strict AML/TF standards,

- insistence on the secrecy of a transaction and similar;

3) Customers where, owing to their structure, it is difficult to identify the beneficial owners or controlling persons, customers with trusts in their structure, customers using third parties, customers where owing to the legal form or complex and unclear relations it is hard to determine the identity of beneficial owners or controlling persons, such as: foundations, trusts and similar persons under foreign law, then voluntary and not-for-profit NGOs, such as legal persons with unclear ownership structure which were not formed by a company from a country adhering to the AML/CFT standards, comparable to the standards stipulated by the Law;

4) Customers performing activities including higher volumes and cash payments (for example: (restaurants, gambling shops, filling stations, exchange offices, casinos, flower shops, precious metal dealers, car dealers, art dealers, transportation services, sports clubs, construction companies, investors in reals estate construction…);

5) Charity and other non-profit organizations, especially if registered abroad, where the flow of money is difficult to trace and which are not under any form of supervision or control;

6) The so called periodic customers – customers with occasional activities which cannot be explained and with significant transactions;

7) Customers with accounts opened with different financial institutions in the same area without apparent economic justification;

8) Customers insisting on quick undertaking of a transaction or business with disregard for higher costs incurred in such ways;

9) Customers offering money, gifts or other favors, values, privileges for services that might be considered suspicious and not fully in compliance with laws;

10) Customers insist that it is not necessary to complete some of the required documents;

11) Customers avoid submitting the required documents or a reporting entity suspects that the submitted documents are complete and correct;

12) Customers performing activities identified in the National risk assessment as bearing high-risk;

13) Customers do not know where the business documentation is kept;

14) Customer has no employees or offices, which is disproportionate to the volume of business;

15) A customer often changes names, registered offices, ownership structures etc.;

16) Private investment funds;

17) Customers often change broker-dealer companies attempting to hide activities on the capital market and financial status or have multiple accounts with different broker-dealer companies;

18) Customers which have not been active, suddenly perform transactions on the capital market in large volumes and values;

19) Customers declare unusual requests for privacy protection, especially regarding information concerning their identity, activity, assets or operations;

20) A customer desists from an order to avoid identification after being acquainted with the obligation to identify themselves pursuant to the provisions of the Law;

21) A customer disregards commission, fees, costs and risk of the transaction;

22) A customer is a newly-founded domestic legal entity with low initial capital investing large amounts of money in trading in securities;

23) A customer has friends or family members working for issuers of securities;

24) Customers for which there is suspicion that they are persons designated on "black lists" (the Consolidated Sanctions List of the Security Council Committee, based on 1267 Resolution of the United Nations Security Council, EU and other lists) or that they are linked to persons on such lists;

25) Media link a customer to terrorism/ terrorism financing/extremism and fundamentalism/religious radicalism;

26) Foreign arms dealers and weapon manufacturers;

27) Non-residents and foreigners;

28) A customer is a Republic of Serbia official, i.e. a person who has held in the last four years a high-level public office in Serbia, such as:

- President of the country, Prime Minister, Minister, State Secretary, Special Advisor to a Minister, Assistant Minister, Secretary of a Ministry, Director of an authority within a ministry and their assistants and Director of an independent organization, as well as their deputies and assistants,

- Member of National Assembly,

- Judges of the Supreme Court of Cassation, Commercial Appellate Court and Constitutional Court,

- President, Vice President and Member of Council of the State Audit Institution,

- Governor, Vice-Governor, member of the executive board and member of the National Bank of Serbia Council of the Governor,

- Person with a prominent office in diplomatic-consular offices (Ambassador, Consul General, Chargé d'Affaires),

- Member of a managing board in a public enterprise or a majority-State-owned company;

- Member of a managing body of a political party;

- A customer that is an immediate family member of a foreign official: Spouse or common-law partners, parents, brothers, sisters, children, adopted and foster children and their spouses or common-law partners,

- A customer that is a close associate of an official, and/or any natural person that has profited from the property/assets or established a business relation or has any other close business relation with the official,

29) A customer is a foreign country official, i.e. a person who has held in the last four years a high-level public office in a foreign country, such as:

- Head of state and/or head of government, member of government and their deputies,

- Elected representative of a legislative authority,

- Judges of Supreme Court, Constitutional Court or other high judicial authority, whose judgments are not subject, save in exceptional cases, to further regular or extraordinary legal remedies,

- Members of courts of auditors, supreme audit institutions or managing boards of central banks,

- Ambassadors, Chargés d'Affaires and Military Attache,

- Member of managing or supervisory bodies of a legal entity in the majority ownership of a foreign state,

- Member of a managing body of a political party,

- A customer who is an immediate family member of a foreign official: Spouse or common-law partners, parents, brothers, sisters, children, adopted and foster children and their spouses or common-law partners,

- A customer that is a close associate of an official, and/or any natural person that has profited from the property/assets or established a business relation or has any other close business relation with the official,

30) A customer is an official of an international organization, i.e. a person who has held in the last four years a high-level public office in an international organization, such as: CEO, deputy CEO, member of managing boards or other equivalent function in an international organization;

31) Foreign financial institutions of countries not adhering to AML/CFT standards, except those founded by the groups from the white list countries;

32) Sporting companies;

33) Customers with residence or registered office in entities not recognized internationally as states (the entities provide options for fictitious registration of a legal persons, facilitate issuance of fictitious identification documents and similar);

34) A customer is a foreign legal person not performing or prohibited from engaging in trading, production or another activity in the state where it is registered (this is the case of a legal person headquartered in the state known as an off-shore financial center and for which certain restrictions apply regarding the performance of registered activity in the state);

35) A customer is a fiduciary or other similar legal arrangement with unknown or concealed owners or directors (a legal arrangement offering representation services to a third person, i.e. company, founded by a concluded contract between the founder and the manager that manages the assets of the founder, to the benefit of certain persons of the beneficiary or for other specific purposes);

36) A customer is a financial organization which is not required to be licensed by a relevant supervisory authority for performance of its activities, and/or pursuant to the national legislation is not subjected to AML and CFT measures;

37) A customer is a non-profit organization (institution, company or other legal person, i.e. established entity not performing economic activities) and meeting one of the following conditions:

- Registered in the state known as an off-shore financial center,
- Registered in the state known as a financial or tax haven,
- Registered in the state that is not a signatory to the Treaty on European Union,
- There is a natural or legal person among its directors or founders, resident in any of the states listed in the previous point,

38) A customer is a foreign legal person established using bearer shares;

39) A customer uses postal codes and postal addresses instead of the address containing a street number and street name or the address and contact information is incorrect or non-existent. (*For example: return mail from nonexistent addresses or the telephone number the customer left at identification is unavailable or non-existing*);

40) Customers performing activities identified in the National risk assessment as bearing high-risk.

(For example, when establishing a business relation a reporting entity assesses the type of customer the entity establishes business relations with. Based on the analysis of previous suspicious activities, types of cases and state risk some forms of companies entail greater ML/TF risk. Specifically, by analysis of previous years and money laundering cases it has been established that all money laundering cases involve limited liability companies, as the most

common form of a company, when persons linked to illegal activities register companies. When assessing risk, a reporting entity must also take into account such circumstances.

A customer is a limited liability company categorized as small legal person registered in the country with a simple ownership structure. A customer mostly deals with cash and has several persons with disposition rights over the funds. A customer might be assessed as carrying moderate risk based on such information at the level of a client. Considering risk at the level of a reporting entity, it is useful to take into account the effects of risk on the reporting entity, that is, consequences of risk on the reporting entity, and the risk category can differ. In this example, if most of the customers of a reporting entity are small or middle legal persons, regardless of their simple ownership structure, the effect on the reporting entity and its reputation could be large and therefore the risk assessment would be high at the level of the reporting entity.

If a reporting entity has customers with complex ownership structures, but their number is inconsiderable or they have no considerable volumes of business, although the customer would entail high risk due to its complex ownership structure, the effect on business of the reporting entity is negligible, and from the aspect of a reporting entity the risk could be categorized as low).

If a customer is a legal person with complex ownership structure, a reporting entity is required to obtain a written statement on reasons for such structure from beneficial owners or customer representatives, to consider whether there are reasons for suspicion of money laundering or terrorism financing, to make an official record thereof, which shall be kept in accordance with the Law.

Moreover, when assessing customer risk, a reporting authority must take into account an appraisal of forms of companies which bear higher risk. When establishing a business relation, a reporting entity must pay special attention to the assessment and analysis of risk of the companies identified in the National Risk Assessment as entailing higher risk.

In addition, persons coming from the non-profit sector must be analyzed with due diligence when assessing terrorism financing risk.

Transaction risk

Increased transaction risk is entailed with the following transactions:

1. Transactions which are outside the normal course of business of the customer;

2. Transactions with no economic justification (e.g. frequent trading in securities, when purchases are performed by placing cash on special purpose accounts, and then soon sold at lower prices – securities trading with a planned loss,

3. Transactions implemented in a way avoiding standard and usual control methods,

4. Transactions encompassing several participants, without an apparent economic purpose, several mutually connected transactions executed over a short period of time or in several consecutive intervals under the designated thresholds for transactions reported to the Administration for Prevention of Money Laundering;

5. Transactions where it is obvious that the customer is trying to conceal the true cause and reason for the transaction;

6. Transactions where the customer refuses to submit documentation;

7. Transactions where the documentation does not match the manner of execution of the transaction;

8. Transactions where the source of funds is not clear or their connection to the operations of the customer cannot be established;

9. Announced block transactions in shares, especially when including newly-formed companies or companies registered in off-shore destinations;

10. Trading in shares on a regulated market, which were the subject of lien following the loans to share owners – acquisition of shares through simulated stock exchange transaction;

11. Transactions which a customer would execute for and on behalf of the person or entity against which there are measures in force introduced by the United Nations or the Council of Europe;

12. Business relations established in favor of the person or entity on the list of persons or entities against which there are measures in force introduced by the United Nations or the EU;

13. Business relations including constant or large payments of money from and/or to the customer's account opened with a credit or financial institution of a non-EU country, i.e. business relations established by a foreign credit/financial or other fiduciary institution headquartered in a non-EU state, on its own behalf and for the account of the customer,

14. Business relations established in customer's absence.

(*For example, when assessing transaction risk one should start with answering the following questions: What is the subject of the transaction? Is the trading in shares on the stock exchange or off the stock exchange? Are shares acquired through a Takeover Bid? Are these FOP (free-of-payment) transactions (gifts, inheritance, court orders)? Is the transaction unusually high taking into account recent transactions of the customer in question*?

The following transactions also entail high risk of money laundering and terrorism financing:

Payments and withdrawals of money from/to the customer's account, other than the customer's account stated when the customer was identified, i.e. it usual business account (especially when involving international payments);

Transactions intended for persons domiciled or registered in a state known as a financial or tax haven,

Transactions intended for persons domiciled or registered in a state known as an off-shore financial center,

Transactions intended for non-profit organizations headquartered in: A country known as an off-shore financial center, or a state known as a financial or tax haven.

For reporting entities supervised by the Securities Commission the following transactions also carry a high level of risk:

1. Frequent trading in securities, when purchases are performed by placing cash on special purpose accounts, and then soon sold at lower prices.

2. Announced block transactions in shares, especially when including unknown or newly-formed companies, and especially companies from off-shore destinations;

3. Purchase of securities using assets deposited in several accounts in several different banks, especially if the deposited funds are just below the designated thresholds for reporting a transaction.

4. A customer invests in liquid securities yielding high returns, but fails to demonstrate interest in their performance or sells the stock without a reason and suddenly.

5. Trading in shares on a stock exchange and off the stock exchange, which were subject to lien, following loans to share owners – simulated stock exchange transactions.

6. A customer shows interest in purchase of securities for large amounts of money without special analyses or advice from an investment adviser and the transaction has no clear financial purpose.

7. Free-of-payment transactions – transfer-of-ownership transactions carried out by broker-dealer companies on behalf of their clients with the Central Securities Depository.

8. Transfer of ownership of shares as gifts to persons who are not related, share gifts from employees to management of the legal entity, transfer of ownership of shares which as a legal basis have court or out-of-court settlements among persons and are in higher amounts, pledge as a consequence of delinquency on approved loans, entry of shares in

order to form legal persons, contracts on merger by acquisition and transfer of ownership of shares among persons in a consortium.

9. A customer often buys or sells shares in amounts slightly below EUR 15,000;

10. Customers which have not been active, suddenly perform transactions on the capital market in large volumes and values.

11. Trading in shares in cases when shareholders give authorizations to third parties to manage their trading accounts and money accounts where there are "linked" money transactions in trading in securities between the owner and such authorized persons.

12. Trading in securities by legal persons from off-shore destinations using custody banks in managing trading accounts or settling transactions.

13. A customer is trying to create an illusion of real trading in securities, but performs fictitious and simulated trading in shares.

14. A customer buys or sells securities in significant amounts immediately before release of news affecting the price of the securities. For example, a customer has never invested in equity, but does it in a favorable moment.

15. A customer trading in securities of low value suddenly buys a significant package of shares and earns considerable profit.

16. A customer participates in pre-arranged and uncompetitive trading in securities, such as WASH sales (fictitious trading) or CROSS trading in illiquid securities or securities with low prices.

17. Sudden trading in securities which were illiquid for longer period of time, through two or more unconnected accounts in a broker-dealer company or more companies.

18. Transactions of one or more connected parties where only one party earns profit while the other loses money.

19. A customer enquiries about quick liquidation of the account, without explanation of the reasons or provides suspicious explanations.

20. A customer signs a fund membership form and buys investment units for larger amounts of money, but fails to demonstrate interest in the performance and operation of the fund, commissions and other expenses or sell the units suddenly and without a reason.

21. After the payment of investment units, a customer terminates the contract demanding pay-outs, although the investment units have an upward trend.

22. Transfer of investment units to third parties by a gift contract, especially if the gifts are for natural persons who are not relatives, and which are economically unreasonable.

23. A customer makes payments into an investment fund from different banks or from the other accounts differing from the one stated in the payment contract or often visits the company and changes payment instructions in the contract regarding the number of account and the bank.

24. An investment fund management company has information that the customer - a natural person makes payments for the purchase of investment units personally and through a large number of other natural persons or through a company of which the person is a founder.

25. A customer requests a transfer of funds accumulated on the individual account of the fund member to a current account of a third person, or to an account in a country which, based on the information from relevant international institutions and the Administration for the prevention of money laundering, fails to apply the AML/TF standards.

26. A customer buys investment units, the value of which is unusually high, relative to the usual purchases of investment units and financial standing of the customer;

27. A customer enquiries about quick redemption of investment units and liquidation of the account, without explanation of the reasons or provides suspicious explanations.

(*For example holder of shares pledges shares for a short-term loan which is paid in cash – illegally obtained money. The pledge is registered with the Central Securities Depository. After the expiration of the loan repayment period and initiation of the pledging procedure, the lender receives the money following the sale of shares on the stock exchange, or if this is not possible, becomes the owner of shares. This secures the legal origin of money, in the amount of shares obtained in such way.*

Disposal of shares owned by small shareholders in the form of a gift to company directors without official compensation, although, in practice, money exchanges hands.

A customer invests significant amounts into securities and then sells them regardless of the fact that their price is rising and requests the transactions to be effected as soon as possible.

The customer buys investment units of a fund from different accounts at different banks and after a short period of time sells them).

<u>Service Risk</u>

Service risk should include the following services:

1) Services new on the market, which have not been previously offered in the financial sector and must be monitored separately to determine the actual risk level;

2) Electronic placement of orders for trading in securities in cases established by reporting entity procedures;

3) Provision of services entailing high risk level as estimated by an employee of the reporting entity;

4) Provision of services by opening a joint account, the assets credited to which come from different sources, which belong to several clients but are deposited to one account opened in one name;

5) Advance payment of services where it is not certain the services will be provided;

6) Services recognized by international legitimate sources as entailing high risk, such as international correspondent banking services (and international) private banking activities;

7) New innovative products or services which a reporting entity does not provide directly, but engages intermediaries or other methods.

(*For example, trading in securities abroad via foreign brokers. In cases of receiving a trading order, money laundering risk is higher with electronic orders or orders made via trading platforms or mobile telephones than with directly placed orders. The probability that the service is used for money laundering or terrorism financing is higher with services of receiving and transmitting securities trading orders than, for example, with investment advice services or portfolio management services).*

When determining the risk level of a customer, business relation, service or transaction in addition to the listed criteria and depending on specific features of their business operations, a reporting entity should take into account the following types of risk and criteria such as:

1. The size, structure and activity of the reporting entity, including the scope, structure and complexity of operations the reporting entity carries out on the market;

2. The status and ownership structure of the customer;

3. Non face-to-face customer, i.e. when the customer is absent at the conclusion of a business relationship or execution of a transaction;

4. The source of assets in a business relation or transaction of a customer that is a politically exposed person (according to the definition from the Law);

5. The purpose of establishing a business relation, service or transaction;

6. Knowing a customer, its experience and knowledge in the area;

7. Other information indicating that a customer, business relation, service or a transaction could entail higher risk.

In order to assess risk, a reporting entity should describe all products, services, contractual relations it enters into and to assess the probability whether the customers would abuse the product/service for money laundering or terrorism financing, and to assess the effect of such probability in a way similar to which it assesses the described customer risk.

2. RISK ANALYSIS

Risk analysis stage is key to risk assessment. The stage of understanding risk follows the stage of identification and description, therefore, analysis is the core part of risk assessment.

After identification of all factors, both internal and external and risk categories, importance of factors is determined and ML/TF risk assessed for each factor. Risk is determined for each factor respectively, in relation to other risk factors and therefore, their effect on the total risk of the reporting entity.

In this phase, apart from the initial, risk list – internal list, external factors should be included – overall environment, political and economic circumstances affecting the work of a reporting entity. In addition, legal framework should be taken into account, availability of public information, earlier experience and experience at the level of the sector and in the National Risk Assessment.

After consideration of all relevant factors, a reporting entity draws a conclusion on risk levels. Reporting entities may use the risk matrix as a method for risk assessment in order to identify low-risk customers, customers entailing higher, but acceptable risk and customers posing high or unacceptable ML/TF risk.

(*For example, a customer may categorize the level of risk in numbers, but still a description must be provided, how a risk has been categorized numerically or, the level of risk can be expressed descriptively: high, low, medium or, there is little probability that a factor is risky, there is medium probability, there is high probability, and there is extremely high probability.*

Moreover, consequences can be expressed as significant, small, irrelevant or of extreme importance. It is on the reporting entity to decide how to express the estimated risk, descriptively or numerically and which matrix will be used.)

When risks are classified, a reporting entity may, taking into account own characteristic features, also define additional levels of risk from money laundering and terrorism financing. The development and formulation of a risk matrix may encompass consideration of different risk categories, such as products and services offered by a reporting entity, customers offered the products and services, size of the institution, its organizational structure etc. The risk matrix can be adapted, changed in accordance with the changes in circumstances of a reporting entity (for example, a broker-dealer company may estimate a customer as entailing low risk, while the same customer may be estimated as high-risk by the accountant, because of the different effects of types of risk and the business relations. The low-risk service in combination with a customer from a foreign country entails higher risk and may be classified as medium risk. If a customer enters into a new business relation, i.e. uses a high-risk service the client risk will change to high-risk.)

Risk analysis comprises analysis of risk relative to the entire operation of a reporting entity, and risk analysis for each group or type of customer i.e. business relationship, or service reporting entity provides within their business activity, or transaction.

The main goal of a risk matrix is the application of a risk-based principle in classification of reporting entities concerning their exposure to ML/TF risk. Based on the information and data from the risk analysis, they are entered into the risk matrix and as a final result, the ML/TF risk level of a reporting entity is determined.

The risk matrix is a tabular overview of information about different types of risk, categorized per activities of a reporting entity, to structural and inherent risk, and overview of effectiveness of the ML/TF risk management by the reporting entity, the trend of the established risk, relative to the previously observed period.

(For example, the structural risk shown in the risk matrix may be established based on the share of a reporting entity in transaction values on the regulated market/OTC market, share of the number of clients in the total number of clients, share of the number of transactions a reporting entity performed in the total number of transactions, and on the basis of information when the reporting entity obtained an operating license, and whether this a newly formed reporting entity. The inherent risk is the level of risk per activities of a reporting entity (broker activities, investment adviser activities and portfolio manager activities, management of open-end or closed-end investment funds), established relative to the total number of clients, classified into natural persons (residents, non-residents and officials) and legal persons (residents and non-residents), the total value of transactions on the stock exchange (per markets, into Prime Listing, Standard Listing, Open Market and MTF) and off the stock exchange (OTC), the total number of customers categorized per geographical risk, to customers from the Republic of Serbia, customers from high-risk areas which are on the lists on international organizations, customers from offshore destinations and other customers. When establishing inherent risk connected with the performing of registered activity of the reporting entity, as a parameter for calculation of share of business activity in

total activities of a reporting entity data may be used on the total profit from operations, categorized into income from broker activities, income from portfolio manager activities, profit from sale and purchase of units of investment funds and other income from regular operations.)

Effectiveness of the ML/TF risk management by a reporting entity is assessed based on the established quality control system and risk management system. And it is observed in terms of the following levels of activities of a reporting entity: Corporate governance, risk management, internal bylaws, internal control, compliance, reporting and training. The main purpose of the activities is to establish an adequate risk control and management system in order to decrease existing risks, and to comprehend and manage potential risks.

The result of the formulation and use of a risk matrix is an appraisal of net risk profile of a reporting entity. The risk matrix is a tool in application of the approach based on risk assessment of a reporting entity, and a reporting entity must take into consideration the information and data when assessing risk of own operations (for example, previously adopted measures by supervisory authorities, reports by authorized auditors, stock exchange information etc.).

In order to assess the exposure of a reporting entity to ML/TF risk, a reporting entity must know each segment of operation where a threat from money laundering and terrorism financing might appear i.e. a reporting entity must assess vulnerability compared to the threat. It is necessary to identify risks at all levels of business operation, from the operating level to the highest management structures and all employees of a reporting entity should be included in the process. The scope and complexity of operation of a reporting entity is vital in establishing vulnerability (for example, a broker-dealer company with a large number of clients conducting on a daily basis a large number of transactions on the stock exchange is more exposed to ML/TF risk compared to another reporting entity with a small number of inactive clients).

A reporting entity assesses the ML/TF risk exposure, the probability of a negative effecting stemming from risks and the effect of risks to the goals of operation.

Money laundering and terrorism financing risk assessment has as a starting point an assumption that different products and services offered and provided by reporting entities, the different transactions they carry out are not equally vulnerable and susceptible to money laundering and terrorism financing abuses. Risk analysis is performed in order to apply control measures commensurate to the recognized risk. This enables reporting entities to focus on those clients, countries, products, services, transactions, methods of operation which pose the greatest risk.

The money laundering and terrorism financing risk assessment aims to pin down the probability of money laundering and terrorism financing. (The risks a reporting entity faces should be analyzed from the viewpoint of determining a probability that something will

occur and from the viewpoint of probable negative effects. For example, what the adverse effect would be when money is of criminal origin or what the fine would be in case of legislation changes, reputation damages to the entity and to the sector and so on.)

3. EVALUATION AND RISK MANAGEMENT

Evaluation and risk management entails effective use of results obtained in risk analysis process. Based on the results, action priorities are defined (*e.g. what risks have been assessed as very important and the urgent risk mitigation activities, to what extent state-level risks are present in the operations of a reporting entity and similar*).

What methods a reporting entity will apply to mitigate risks is on the entity to decide (*to prohibit the use of a service or product, greater attention paid to certain transactions, capacity building etc.*).

High risk requires immediate attention, without delay. Medium risks require ASAP actions, while lower risks should be monitored.

Risk assessment contains all the measures to be undertaken and their priority. They should be assessed when planning business activities and the resources necessary for the following year (*e.g. assets required for training for the following year, as it has been observed that although most of the employees should be knowledgeable about money laundering and terrorism financing they do not possess adequate levels of understanding and knowledge, or it is necessary to enhance cooperation among organizational units and in what ways the cooperation would be enhanced*).

Money laundering and terrorism financing risk is specific to each reporting entity and it requires adequate management approach, tailored to the level and structure risk and the volume of business. The goals and principles of money laundering and terrorism financing risk management should enable reporting entities to determine appropriate business policy and procedures, including rules on general customer due diligence actions and measures applied, promoting high ethical and professional standards and preventing the misuse of business activities of a reporting entity for criminal activities.

It is on management to steer the business policy by formulating goals and making strategic decisions. It is on management to take into account money laundering and terrorism financing risks when finalizing business plans and policies.

Documenting risks and method of presentation of risks is essential to the decision-making process and planning. For these reasons, the management should be involved from

the start into preparation and analysis of money laundering and terrorism financing risks and to put in place appropriate control systems.

(For example, it is important to have a system in place which will reject business relations with customers for which there is not enough information nor prior record. Moreover, it should be taken into consideration that money laundering and terrorism financing risks should be taken into account in the development phase of introducing a new service or product. It is necessary that members of the management have sufficient power to make and implement required decisions in practice).

The purpose of the measures to prevent criminal assets or money intended for terrorism to enter the reporting entity. Risk mitigation measures are to recognize certain behaviors in a reporting entity, which would lead to timely reporting of suspicious activities.

In addition, the management must promote ethical business conduct and support ethical behavior. Ethical behavior entails professional and individual responsibility of employees for the decisions they make and activities undertaken in their work.

RESULTS OF RISK ASSESSMENT

When all the phases are completed and risks are determined, the results should be documented. As already indicated, it is necessary to make a decision at the very beginning of the process who will participate in the process, how the information will be collected, the methods to be used. Results should be then listed in a document containing definitions of terms used, methodologies described and most importantly the results of risk assessment. It is important that results are visible and the way how the results were reached. Also, it should state in what way the state-level risks affect the reporting entity.

When risks are analyzed and determined, a money laundering and terrorism financing risk strategy should be applied. It enables a reporting entity to implement internal policies and procedures for risk mitigation and risk elimination, with the intention to remove any risks to harm the reputation of the reporting entity, eliminate operation risks, risks from compromising own integrity and reputation following a sanction by a supervisory authority and so on.

Management approves the internal policies and procedures and they apply to all employees in a reporting entity. Risk appraisal and development of adequate policies and procedures provide for continuity in ML/TF risk management in spite of all changes which might occur in management and employee structures.

The established business policies and procedures should enable effective management of recognized risks and their mitigation. A reporting entity is to focus on the area of operation mostly susceptible to different types of misuse in order to prevent money laundering and terrorism financing. The higher the risk, the higher number of control measures need to be implemented. For example, a reporting entity may introduce limitation mechanisms for high-risk products or provide that a transaction requires prior management approval etc.

Special policies and procedures must be introduced at the level of a reporting entity, for actions and measures (due diligence) for the prevention and detection of money laundering and terrorism financing.

DUE DILIGENCE FOR DETECTION AND PREVENTION OF MONEY LAUNDERING AND TERRORISM FINANCING

As described, following the analysis of money laundering and terrorism financing risks (Article 6 of the Law), when performing their registered activities, reporting entities must act in accordance with the statutory obligations and implement the following actions and measures (due diligence) for the prevention and detection of money laundering and terrorism financing, prior, in the course of and after a transaction or establishing a business relation:

1) customer due diligence;

2) sending information, data, and documentation to the Administration for Prevention of Money Laundering (APML);

3) designating persons responsible for complying with the obligations laid down in the Law (compliance officers) and their deputies, and providing conditions for their work;

4) regular professional education, training and capacity building of employees;

5) providing for regular internal control of complying with the obligations laid down in the Law, and internal audit if in accordance with the scope and nature of business operations of the reporting entity;

6) developing a list of indicators for identifying persons and transactions with respect to which there are reasons to suspect money laundering or terrorism financing;

7) record keeping, protection and retention of data from such records;

8) implementing measures laid down in the Law by reporting entity branches and majority-owned subsidiaries located in foreign countries;

9) implementing other actions and measures based on the Law.

1. CUSTOMER DUE DILIGENCE (Knowing a customer and monitoring their business transactions)

Identifying and verifying the identity of a customer

Prior to establishing business relations or executing a transaction exceeding the amount provided for by the Law or in other cases set forth in the Law (the designated threshold), reporting entity must obtain the necessary information about the customer in order to identify and verify their identity.

It is possible to properly identify and verify the identity of a customer exclusively by inspection of valid, independent and objective sources, such as the official identification document or other official documents (personal document, official identification document, original or certified documents from a register, obtaining information directly from the customer) proving identity of the customer (natural person, legal person, legal representative, procura holder or empowered representative, foreign law person, entrepreneur, civil person, and establishing and verifying the identity of a natural person by a qualified electronic certificate).

In cases when the identity of a customer is not possible to establish or verify and when it is not possible to determine who the beneficial owner of the customer is and when it is not possible to obtain information about the purpose and intended nature of a business relation or a transaction or other information in accordance with the Law, a reporting entity must refuse to establish a business relation and refuse to participate in transactions and must terminate the existing business relations with the customer (Article 7 of the Law). Depending on the ML/FT risk level entailed, the international standards and the Law allow reporting entities to execute three types of customer due diligence – general, simplified and enhanced customer due diligence.

Identification of the beneficial owner of a customer

A reporting entity must identify the beneficial owner of a customer that is a legal person or person under foreign law by obtaining the data referred to in Article 99, paragraph 1, item 13 of this Law: name and surname, date and place of birth and permanent or temporary residence of the customer's beneficial owner.

A reporting entity must obtain such information by inspecting the original or a certified copy of the documentation from the register maintained by the competent authority in the country where the customer has a registered office, with no more than six months having elapsed from the date they were issued, a photocopy of which the entity must keep in accordance with the law. A reporting entity must indicate, on its copy, the date, time, and the name of the person who inspected the original or a certified copy thereof. The data may be also obtained by directly accessing the official public register in accordance with the provisions of Article 20, paragraphs 4 and 6 of the Law.

For example, if a reporting entity is to obtain such information, it may inspect the documents kept by the Business Registers Agency or by other competent authorities of the country in which the customer has a registered office. The documents pertaining to identification and verification of identity of a legal person shall be issued no earlier than three months before its inspection, while the documents pertaining to identification and verification of identity of a beneficial owner of the legal entity and person under foreign law shall be issued no earlier than six months before its inspection. The information may be also obtained by directly accessing the official public register. A print-out shall contain the relevant information, date, time and personal name of the person who inspected the documents and it shall be retained in accordance with the law.

If it is not possible to obtain all the information about the beneficial owner of a customer from the official public register or the register maintained by the competent body of the country where the customer has a registered office, the reporting entity must obtain the missing information from the original or a certified photocopy of the document or other business documentation submitted by the representative, procura holder or empowered representative of the customer. If, for objective reasons, the information cannot be obtained as stated, the reporting entity must obtain it by accessing commercial and other available databases and sources of information, or from a written statement given by the representative, procura holder or empowered representative and beneficial owner of the customer. When identifying the beneficial owner, the reporting entity may obtain a photocopy of a personal document of the beneficial owner of the customer.

The reporting entity shall undertake reasonable measures to verify the identity of the beneficial owner of a customer as to know at any time the ownership and management structure of the customer and its beneficial owners.

If, after all the stipulated actions, the reporting entity is still unable to identify the beneficial owner, it shall identify one or more natural persons who hold top management positions with the customer.

A reporting entity must substantiate all the actions and measures undertaken regarding identification of the beneficial owner of a customer.

The requirement of identification of the beneficial owner of a customer includes natural persons. This means that a beneficial owner of a customer who is a natural person is the natural person who directly or indirectly controls the customer. Control of a customer entails control of a transaction or of a business relation resulting in a fact that the customer is not acting on its own behalf. For example, if a customer who is a natural person establishes a business relationship or executes a transaction in the presence of another person giving instructions or executes a transaction by reading a note with instructions etc. then there is suspicion that another person controls the customer - natural person.

Moreover, the procedure for establishing a beneficial owner of a customer is explained in more detail in the Guidelines for Application of the Law on Prevention of Money Laundering and Terrorism Financing in the part pertaining to identification of beneficial owners.

General Customer Due Diligence

Customer due diligence represents a key preventive element in detecting and preventing money laundering and terrorism financing. The purpose of executing due diligence is to identify and verify the real identity of a customer and it encompasses the following activities: Identification of a customer and verification of its identity, identification of the beneficial owner of the customer, if the customer is a legal person, obtaining information about the intended purpose and nature of the business relation, service or transaction and other information in accordance with the provisions of Article 7 of the Law.

A reporting entity carries out due diligence (actions and measures) referred to in Article 7 of the Law in the following cases: When establishing a business relation; when carrying out transactions above the applicable designated threshold of EUR 15000 or more in dinar equivalent at the National Bank of Serbia official middle exchange rate, on the day of transaction, irrespective of whether the transaction is carried out in one or more than one connected operations; when there are reasons for suspicion of money laundering or terrorism financing with respect to a customer or transaction, regardless of the value of the transaction, and when there are doubts about the veracity or adequacy of previously obtained information about a customer or beneficial owner (Article 9 of the Law).

A reporting entity identifies and verifies the identity of a customer based on credible, independent and objective sources by inspecting a relevant identification document which is an official document, original or a certified copy of the decision of the company register, directly in the presence of the customer or its legal representative or an empowered representative (when the customer is a legal person) or indirectly through a third person.

It shall be unlawful to establish a business relationship or execute a transaction in cases when the identity of a customer is not possible to establish, or when an obligor suspects the veracity of information or documents provided, furthermore, in situations when the customer is not ready or willing to cooperate with the reporting entity in determining the true and complete information required within the customer due diligence. In such cases, a business relation must not be established and an already existing relationship or a transaction must be terminated and the APML notified thereof.

When establishing a relationship with a customer, a reporting entity must, in addition to applying customer due diligence actions and measures, obtain the following information:

1) business name and legal form, address, registered office, registration number and tax identification number (TN) of the legal entity or entrepreneur which establishes a business relation or carries out a transaction, or the one for which a business relationship is established or a transaction conducted;

2) name and surname, date and place of birth, permanent or temporary residence, unique personal number of a representative, empowered representative or procura holder, who in the name of or on behalf of a customer - a legal person, a person under foreign law, a company service provider, an entrepreneur, or a person under civil law, establishes a business relationship or conducts a transaction, as well as the type and number of their identity document, its date and place of issue;

3) name and surname, date and place of birth, residence or domicile, personal identification number of the natural person, of the representative or empowered representative, or entrepreneur who establishes a business relation or carries out a transaction, or the one for which a transaction is conducted or business relation established, and the type and number of the personal identification document, date and place of issuing;

4) Purpose and intended nature of a business relation, and information on the type of business and business activities of a customer;

5) Date of establishing a business relationship (date of the contract on opening and management of a securities account, date of the contract on provision of investment services, date of joining an investment fund etc.);

6) name and surname, date and place of birth and permanent or temporary residence of the customer's beneficial owner;

7) Name of the persons under civil law.

A reporting entity must obtain the following information when carrying out a transaction amounting to the RSD equivalent of EUR 15,000 or more, in addition to due diligence:

1) business name and legal form, address, registered office, registration number and tax identification number (TN) of the legal entity or entrepreneur which carries out a transaction, or the one for which a transaction is conducted;

2) name and surname, date and place of birth, permanent or temporary residence, unique personal number of a representative, empowered representative or procura holder, who in the name of or on behalf of a customer - a legal person, a person under foreign law, an entrepreneur, trust, or a person under civil law, conducts a transaction, as well as the type and number of their identity document, its date and place of issue;

3) name and surname, date and place of birth, residence or domicile, personal identification number of the natural person, of the representative or empowered representative or entrepreneur who carries out a transaction, or the one for which a transaction is conducted, and the type and number of the personal identification document, date and place of its issuing;

4) Date and time of the transaction;

5) Amount and currency of the transaction;

6) The intended purpose of the transaction, name and surname, the place of permanent residence i.e. business name and headquarters of the intended recipient of the transaction;

7) The method of conducting the transaction (stock exchange trading, block transaction on the stock exchange, takeover bid, purchase/sale of investment units etc);

8) Name and surname, date and place of birth and permanent or temporary residence of the customer's beneficial owner;

9) Name of the persons under civil law.

When there are reasons for suspicion of money laundering or terrorism financing with respect to a customer or transaction, and when there are doubts about the veracity or adequacy of previously obtained information about a customer or beneficial owner, a reporting entity must obtain all the information referred to in Article 99, paragraph 1 of the Law, as a part of the customer due diligence:

1) business name and legal form, address, registered office, registration number and tax identification number (TN) of the legal entity or entrepreneur which establishes a business relation or carries out a transaction, or the one for which a business relationship is established or a transaction conducted;

2) name and surname, date and place of birth, permanent or temporary residence, unique personal number of a representative, empowered representative or procura holder, who in the name of or on behalf of a customer - a legal person, a person under foreign law, a company service provider, an entrepreneur, or a person under civil law, establishes a business relationship or conducts a transaction, as well as the type and number of their identity document, its date and place of issue;

3) name and surname, date and place of birth, residence or domicile, personal identification number of the natural person, of the representative or empowered representative, or entrepreneur who establishes a business relation or carries out a transaction, or the one for which a transaction is conducted or business relation established, and the type and number of the personal identification document, date and place of issuing;

4) Purpose and intended nature of a business relation, and information on the type of business and business activities of a customer;

5) Date of establishing a business relationship;

6) Date and time of the transaction;

7) Amount and currency of the transaction;

8) The intended purpose of the transaction, name and surname, the place of permanent residence i.e. business name and headquarters of the intended recipient of the transaction;

9) The manner in which a transaction is executed;

10) Information and data about the origin of property which is underlying or will underlie a business relation or a transaction;

11) Information about the existence of reasons for suspicion of money laundering or terrorism financing;

12) Name and surname, date and place of birth and permanent or temporary residence of the customer’s beneficial owner;

13) Name of the persons under civil law.

A reporting entity must collect information about the origin of property which is or will be the subject of a business relationship, or of transaction where the business relationship has not been established, and assess the credibility of the collected information if, in line with the risk analysis it establishes that in relation to the customer ML/TF risk is high.

A reporting entity collects information about the origin of assets from a customer and, undertaking reasonable measures, additionally verifies the information through available sources (for example: bank account statement, sale contract, inheritance documents etc).

The Law is based on the assumption that certain customers, business relations, products or transactions entail higher risk while the other entail lower risk of money laundering or terrorism financing. In some cases, the Law requires strict due diligence procedures or however, allows simplified due diligence. In addition to the regular due diligence the Law stipulates two different methods to conduct due diligence, as follows: Enhanced due diligence of a customer where there is high risk of money laundering and terrorism financing and simplified customer due diligence allowed in cases when there is inconsiderable risk of money laundering and terrorism financing.

Simplified Customer Due Diligence

The Law provides that a reporting entity can conduct simplified or reduced due diligence measures in cases referred to in Article 42 of the Law. This means that a reporting entity identifies and verifies the identity of its customer and monitors the customer activities, but the procedure is less complex.

Simplified customer due diligence can be applied in cases when the customer is:

1. a reporting entity (according to the Law) or the entity or person from a foreign country on the list of countries that apply international standards in the area of prevention of money laundering and terrorism financing at the European Union level or higher:

- a bank;
- an authorized exchange office;
- business entities performing money exchange operations based on a special law governing their business activity;
- investment fund management companies;

- voluntary pension fund management companies;
- financial leasing providers;
- insurance companies, insurance brokerage companies, insurance agency companies and insurance agents with a license to perform life insurance business, except for insurance agency companies and insurance agents for whose work the insurance company is responsible according to the law;
- broker-dealer companies;
- e-money institutions;
- payment institutions;
- public postal service operator headquartered in the Republic of Serbia, established in accordance with the law governing postal services;

2. a state body, body of an autonomous province or municipality, public agency, public service, public fund, public institute or chamber;

3. a company whose issued securities have been admitted to trading on a securities market in the Republic of Serbia or in a country applying the international filing standards at the European Union level or higher;

4. a person representing low risk of money laundering or terrorism financing, based on the risk assessment.

A reporting entity may apply simplified customer due diligence when it assesses that the nature of the business relationship, form or method of transaction, customer business profile, or other circumstances related to the customer, pose insignificant or low ML/TF risk.

When applying simplified customer due diligence, a reporting entity must implement an adequate level of monitoring of business operations of the customer, to be still able to detect any unusual and suspicious transactions.

In cases where simplified customer due diligence actions and measures are applied, a reporting entity must obtain the following information:

When establishing a business relationship:

1. business name and legal form, address, registered office, registration number and tax identification number (TN) of the legal entity or entrepreneur which establishes a business relation, or the one for which a business relationship is established;

2. name and surname, date and place of birth, permanent or temporary residence, unique personal number of a representative, empowered representative or procura holder, who in the name of or on behalf of a customer - a legal person, a person under foreign law, an entrepreneur, trust, or a person under civil law, establishes a business relationship, and the type and number of their identity document, its date and place of issue;

3. name and surname, date and place of birth, permanent or temporary residence, personal identification number of the natural person, of the representative or empowered representative, or entrepreneur who establishes a business relation, or the one for which a business relation is established and the type and number of the personal identification document, date and place of issuing;

4. purpose and intended nature of a business relation, and information about the type of business and business activities of a customer;

5. Date of establishing a business relationship;

6. Name and surname, date and place of birth and permanent or temporary residence of the customer's beneficial owner (except when the customer is a state or public authority or a company with listed securities);

7. Name of the persons under civil law.

When carrying out a transaction:

1. business name and legal form, address, registered office, registration number and tax identification number (TN) of the legal entity or entrepreneur which carries out a transaction, or the one for which a transaction is conducted;

2. name and surname, date and place of birth, permanent or temporary residence, unique personal number of a representative, empowered representative or procura holder, who in the name of or on behalf of a customer - a legal person, a person under foreign law, an entrepreneur, trust, or a person under the civil law, conducts a transaction, and the type and number of their identity document, its date and place of issue;

3. name and surname, date and place of birth, permanent or temporary residence, personal identification number of the natural person, of the representative or empowered representative or entrepreneur who carries out a transaction, or the one for which a transaction is conducted, and the type and number of the personal identification document, date and place of its issuing;

4. Date and time of the transaction;

5. Amount and currency of the transaction;

6. The intended purpose of the transaction, name and surname as well as the place of permanent residence i.e. business name and headquarters of the intended recipient of the transaction;

7. The manner in which the transaction is executed;

8. Name and surname, date and place of birth and permanent or temporary residence of the customer's beneficial owner (except when the customer is a state or public authority or a company with listed securities);

Enhanced Customer Due Diligence

In cases when a customer, business relation, service or transaction are categorized as high ML/FT risk, in addition to general due diligence, enhanced customer due diligence must be applied.

The Law defines that the enhanced customer due diligence is applied when establishing a correspondent relationship with banks and other similar institutions from foreign countries, when implementing new state of the art technology and services, when establishing a business relationship or carrying out a transaction if the customer is an official, when a customer is not physically present when establishing and verifying their identity, when a customer or a legal person appearing in the customer's ownership structure is an off-shore legal person, when establishing a business relationship or carrying out a transaction with a customer from a country which has strategic deficiencies in the system for prevention of money laundering and terrorism financing.

In addition, a reporting entity must apply enhanced customer due diligence when it assesses that the nature of the business relationship, form or method of transaction, customer business profile, or other circumstances related to the customer, pose or might pose high ML/TF risk.

In those cases, the Law provides for the special scope of due diligence with special focus and application of additional measures.

A reporting entity must define (in an internal enactment) which enhanced customer due diligence and to what extent will be applied in specific situations.

New technologies and new services

A reporting entity must assess the risk of money laundering and terrorism financing in relation to a new service it provides within the scope of its business, new business practice, and the methods for providing new services, before it introduces such services.

A reporting entity must assess the risk of using modern technologies in the existing or new services.

A reporting entity must pay special attention to any ML/TF risk which might stem from the application of new technologies that allow for abuse of customer's identity (such as for example electronic orders for purchase and sale of securities, orders made via trading platforms or mobile telephones, password abuses, banking services and products which include investments in investment funds as a form of savings etc.) and develop policies and undertake measures for prevention of the usage of new technologies for money laundering and terrorism financing. The policies and procedures of a reporting entity applying to business relations or transactions with absent customers, also apply to doing business with customers using new technologies, in accordance with provisions of Article 37 of the Law.

Official

Pursuant to the Law, an official as a politically exposed person represents a high risk customer. Therefore, reporting entities must apply due diligence in all cases when such a person is a customer, defined as the politically exposed person in accordance with the criteria from the Law and the Guidelines, prior to establishing a business relation or executing a transaction.

A reporting entity is required to establish a procedure for determining whether a customer or the beneficial owner of a customer is an official.

If a customer or the beneficial owner of a customer is an official, the reporting entity must in addition to the actions and measures referred to in Article 7, paragraph 1 of the Law, the following additional actions and measures from Article 38 must be implemented:

1. Obtaining information about the origin of funds and property that is the subject of business relation or transaction from documents submitted by the customer. If it is not possible to obtain the information as described, the reporting entity shall take a statement of origin directly from its customer,

2. Obtaining information about the total property owned by the official,

3. Ensuring that employees of the reporting entity establishing a business relationship with an official must, before establishing such a relationship, obtain written consent from the top management;

4. Monitoring with special attention the transactions and other business activities of an official for the duration of the business relationship.

A reporting entity must obtain information about whether the person in question is an official or not, from a special signed written statement which the customer completes before establishing a business relation or executing a transaction. The written statement must be drawn up in Serbian and English for foreign officials and officials from international organizations and the reporting entity suggests the signing to each customer.

The written statement shall contain at least:

1) Full name, permanent residence, date and place of birth of the customer establishing a business relation or requesting a transaction, the number, type and issuer of the valid identity document,

2) A statement whether the person is a politically exposed person or not – pursuant to the criteria set out in the Law,

3) Information about the type of the political exposure (a person which has been in a prominent public position for the last 4 years, or a family member of a politically exposed person or a close associate of a politically exposed person,

4) Information about the time period of discharging the function, if the customer is a person in a prominent public position for the last 4 years,

5) Information about the type of the public function a person has been performing,

6) Information about family relations, if the customer is a family member of a politically exposed person,

7) Information about the type and manner of business cooperation, if the customer is a close associate of the person,

8) Provision according to which, in order to establish veracity of information, the customer permits the reporting entity to check the information about the customer by inspection of public or other available sources of information, i.e. to acquire such information directly from the competent authorities of another state, consular representative office or embassy of the state in the Republic of Serbia or the Ministry of Foreign Affairs of the Republic of Serbia,

9) Personal signature of the customer.

A reporting entity may acquire information by inspection of public and other available information (reporting entities decide to what degree they will consider the

publicly available information about politically exposed persons accurate and relevant), and the information can be validated with the following authorities: Anti-Corruption Agency, competent state authorities of foreign countries, consular representative offices or embassies of foreign states in the Republic of Serbia i.e. the Ministry of Foreign Affairs of the Republic of Serbia and other publicly available data bases.

When collecting information and analyzing risk, a reporting entity may indirectly discover that a person is a politically exposed person. (*For example, if a customer is a legal person whose securities are listed on the stock exchange, categorized as low risk, but it is determined that its beneficial owner is an official, a high risk customer according the Law, enhanced due diligence must be applied for this person.)* A reporting entity must at all times take into account the merging of risks and their effect on each other.

If a reporting entity establishes that a customer or a beneficial owner of the customer has become an official during their business relationship, the entity must apply all the stated actions and measures. In addition, a written approval must be obtained from the top management for continuation of the business relationship with such person.

Identifying and verifying the identity of a customer, non-face-to-face customer

In the course of identification and verification of identity, reporting entities must apply enhanced customer due diligence measures in cases when a customer or its legal representative is not present.

In addition to the general customer due diligence actions and measures (Article 7 of the Law), a reporting entity is required to undertake some of the following additional measures:

Obtaining documents, information or data based on which an obligor may check and verify the veracity of identification documents and information based on which the identity of the customer was established (copies of cards of current accounts, giro accounts and foreign currency accounts),

2. Additional scrutiny of obtained information about the customer in public and other available data bases,

3. Ensuring that, the first payment to the account opened with the reporting entity is carried out from the account the customer opened with a bank or a similar institution, before execution of other customer transactions,

4. Acquiring relevant references from financial institutions the customer has established business relations with,

5. Additional scrutiny of data and information about the customer in the state of residence of the customer or of its headquarters,

6. obtaining information on the reasons for absence of the customer,

7. Establishing direct contact with a customer by telephone or visiting an authorized person of the reporting entity at home or headquarters of the customer.

When establishing a business relation in customer's absence, where a third person has identified and verified the customer's identity, a reporting entity must ensure that the third person delegated to apply enhanced customer due diligence measures, has established and verified the identity of the customer in their presence.

Off-shore legal person

A reporting entity must set out a procedure for establishing whether a customer or a legal person in the ownership structure of the customer is an off-shore legal person. If so, a reporting entity must, in addition to general due diligence, undertake additional measures and establish reasons for the business relationship, or a transaction in the amount of EUR 15,000 or more, when the business relationship has not been established in the Republic of Serbia, and additionally inspect data about the ownership structure of the legal person. If the customer is a legal person with a complex ownership structure, a reporting entity must obtain a written statement on the reasons for the existence of such a structure, from the beneficial owner or legal representative of the customer. A reporting entity must consider whether there are reasons for suspicion of money laundering or terrorism financing and make an official note, retaining it in accordance with the law.

Countries not implementing international standards in the area of the prevention of money laundering and terrorism financing

When establishing a business relationship or carrying out a transaction amounting to EUR 15,000 or more, in cases when a business relationship has not been established, with a customer from a country which has strategic deficiencies in the system for prevention of ML/TF, a reporting entity must apply enhanced customer due diligence.

The strategic deficiencies primarily include:

1) country's legal and institutional framework, especially criminalization of criminal offenses of money laundering and terrorism financing, customer due diligence, provisions governing data retention, reporting of suspicious transactions, powers and procedures of the relevant state authorities in relation to money laundering and terrorism financing;

2) effectiveness of the system for combating money laundering and terrorism financing in eliminating money laundering and terrorism financing risks.

In such cases a reporting entity must: apply enhanced customer due diligence appropriate to the high risk the customer entails, obtain information about the origin of property which is or will be the subject of the business relationship, or of transaction, obtain additional information on the purpose and intended nature of the business relationship or transaction, conduct additional inspection of submitted identity documents, and undertake other measures in order to eliminate risks.

A reporting entity must act in accordance with the measures issued by the competent state authorities which can determine that doing business with a state which has strategic deficiencies in its system for the prevention of money laundering and terrorism financing bears special risk and forbid the financial institutions they license to form branches and business units in such states; prohibit the establishment of branches and business units of financial institutions from such states in the Republic of Serbia; limit financial transactions and business relationships with customers from such states; require financial institutions to assess, alter or terminate business relations with financial institutions from such states.

Other high-risk customers

Enhanced due diligence measures can be applied in other cases of high risk customers, business relations, services or transactions when a reporting entity estimates that high level of ML/FT risk might exist.

Customers which, considering the experience of the reporting entity, pose high ML/FT risk may be the persons for which the APML has instructed the reporting entity to monitor all transactions or business operations of such persons for which there is reasonable suspicion that ML and FT is involved (Article 76 of the Law), persons for which the APML has

instructed the reporting entity to suspend their transactions (Article 75 of the Law), and persons for which the reporting entity has submitted information to the APML as considering the person or their transactions there were reasons to suspect ML or FT.

The enhanced customer due diligence might include:

1. Mandatory prior written approval for establishing a business relation or execution of a transaction by a person in charge,

2. Mandatory application of one of the following measures:

a) Obtaining documents, information or data based on which a reporting entity additionally checks and verifies identification documents and information based on which the customer's identity was established and verified,

b) Additional scrutiny of obtained information about the customer in public and other available data bases,

c) Acquiring relevant references from relevant institutions the customer has established business relations with;

d) Additional scrutiny of data and information about the customer with the competent state authorities or other competent institutions in the state of residence of the customer or of its headquarters,

e) Establishing direct contact with a customer by telephone or by a visit of an authorized person of the reporting entity at home or headquarters of the customer,

3. Mandatory monitoring of transactions or other business activities a customer carries out with the reporting entity.

Outsourcing some customer due diligence actions and measures

When establishing a business relation, under the conditions laid down by the Law, an obligor may delegate the due diligence measures referred to in Article 7, paragraph 1, to third persons whereby it must check first whether the third person meets the conditions (Article 25 of the Law).

The third person must promptly deliver to the reporting entity, at its request, copies of identification documents or other documentation of customer due diligence measures it has applied.

If the reporting entity questions the credibility of applied customer due diligence actions and measures, or the veracity of data obtained about a customer, it shall undertake additional measures to eliminate the reasons for suspicion and consider whether here is suspicion of money laundering or terrorism financing.

If a third person conducts customer due diligence on behalf of a reporting entity, the reporting entity shall continue to have liability for the applied customer due diligence measures.

A reporting entity cannot accept customer due diligence actions and measures conducted by a third party, if such a person has identified and verified the identity of a customer without the customer's presence, if the customer is an off-shore legal person or an anonymous company.

A reporting entity shall not outsource to a third party to perform customer due diligence actions and measures, if the third party is from a country which has strategic deficiencies in the system for the prevention of money laundering and terrorism financing.

MONITORING CUSTOMER BUSINESS ACTIVITIES

The purpose of monitoring customer business transactions

Regular monitoring of customer business transactions represents a key element in establishing efficiency of implementation of stipulated measures for detecting and preventing money laundering and terrorism financing. The purpose of monitoring customer business transactions is to determine legality of customer operations and check compliance with the intended nature and purpose of the business relation, the customer established with the reporting entity, and its normal scope of business. Customer business transactions are monitored on a scale and with frequency corresponding to the risk perceived and includes the following measures the reporting entity executes:

Obtaining information about all transactions from the moment when the business relationship was established,

Monitoring and ensuring that customer business transactions are consistent with the intended nature and purpose of the business relation,

Monitoring and ensuring that the source of funds of the customer is consistent with the source of funds the customer has stated at the establishment of a business relation with the reporting entity,

Monitoring and ensuring that customer business transactions are consistent with its normal scope of business,

Monitoring and updating documents and information obtained about the costumer.

The following measures are used in monitoring and ensuring that customer business transactions are consistent with the intended nature and purpose of the business relation established with the reporting entity:

Analysis of information about the purchase and/or sale of securities and other financial instruments i.e. other transactions, for a period of time, determining whether there are circumstances for suspicion of money laundering or terrorism financing regarding a purchase or sale of securities/financial instruments or other transactions (for example, if transactions are conducted in smaller amounts below the reporting threshold, and in a shorter period of time). Determining how suspicious a customer, transaction or a business relation is, is founded on suspicion criteria set in the List of Indicators developed for the recognition of persons and transactions with respect to which there are reasons for suspicion of money laundering and terrorism financing,

Updating the previous appraisal of the customer risk level i.e. preparation of a new appraisal of the customer risk level.

When monitoring and ensuring that customer business transactions are consistent with their normal scope of business the following is taken into account:

Monitoring the value of purchase or sale of securities/financial instruments, i.e. other transactions exceeding a threshold – reporting entities decide for themselves what the amount is for each customer separately considering their risk category (for implementation of this measure a reporting entity may establish an appropriate IT system support),

When monitoring and updating documents and information obtained about a costumer, reporting entities undertake the following measures:

The repeated annual customer due diligence, one of the measures of customer due diligence is applied pursuant to Article 34 of the Law,

The repeated customer due diligence, when there is suspicion of veracity of previously obtained information about the customer or beneficial owner (if the customer is a legal person),

Checking information about the customer or its legal representative in a public register,

Checking obtained information directly with the customer or its representative or empowered representative,

Checking the lists of persons, states and other entities against which there are measures in force introduced by the United Nations or the European Union or other relevant institutions.

The scope of monitoring customer business activities

How often and to what extent a customer's activities will be monitored depends on the level of risk a customer entails, i.e. its risk category appraisal. The appropriate level of monitoring of business activities of a customer entails stipulated measures for monitoring business activities of a customer in a continuous manner and considering services and transactions that the reporting entity provides and executes for the customer.

Measures for monitoring business activities of a customer are not required if the customer has had no business activities (for example: if the customer only concluded a contract on opening and managing a securities account or a contract on the provision of investment services, but without any purchase or sale of securities or other transactions) at the conclusion of a business relation.

A reporting entity will implement measures for monitoring business activities of a customer at the time of first sale or purchase of securities/financial instruments, or at the time of other transaction, in conformity with the determined level of risk of the customer, in accordance with the Law, Guidelines and the risk analysis performed by the reporting entity.

In accordance with its ML/FT risk management policy, a reporting entity may opt for more frequent monitoring of business activities of certain categories of customers and adopt additional scope of measures for the monitoring of customer business activities and determining compliance of its operations, in its internal enactments.

2. FILING INFORMATION TO THE ADMINISTRATION FOR PREVENTION OF MONEY LAUNDERING

Within their statutory authority, reporting entities must ensure full cooperation with the competent authorities – the Securities Commission and the Administration for Prevention of Money Laundering (APML). The cooperation among reporting entities and supervisory authorities is obligatory, especially in cases of submitting documentation and

requested information with respect to customers and transactions when there is suspicion of money laundering and terrorism financing. The cooperation is also vital when reporting on all activities and circumstances which might have been connected with money laundering or terrorism financing.

Whenever there is suspicion regarding a transaction or a customer of money laundering or terrorism financing, reporting entities are required to file with the Administration for Prevention of Money Laundering such information, in the manner, form and within the time period stipulated by the Law and the rulebook of the Administration for Prevention of Money Laundering governing methodology for activities in accordance with the Law. Reporting entities have the duty of reporting in cases when they are not able to identify or verify the identity of a customer at conclusion of a business relation or before execution of a transaction as stipulated by the Law, i.e. when the identity of a beneficial owner is not possible to determine or to obtain information about the purpose and intended nature of the business relation or transaction and other stipulated information.

Employees of a reporting entity who find that there are reasons to suspect money laundering or terrorism financing must notify thereof the compliance officer or deputy compliance officer. Reporting entities must organize a procedure for reporting suspicion transactions among all organizational units and authorized persons in accordance with the following instructions:

- Regulate in detail the manner in which reporting is conducted (by telephone, telefax, secured electronic reporting etc.),
- Determine the type of information reported (information about the customer, reasons to suspect money laundering etc.),
- Determine how organizational units cooperate with the compliance officer,
- Determine the customer handling procedure in cases of suspension of a transaction by the APML,
- Determine the role of the person responsible in a reporting entity when reporting a suspicious transaction,
- Prohibit tipping off/disclosing that information, datum or a document will be submitted to the APML,
- Determine measures regarding the continuation of cooperation with the customer (suspension of operation, termination of business relation, enhanced due diligence measures and know-your-client procedures and monitoring future business activities of the customer and similar).

3. PREVENTION OF MONEY LAUNDERING AND TERRORISM FINANCING COMPLIANCE OFFICER

Reporting entities must have a compliance officer and a deputy compliance officer.

The compliance officer carries out the following tasks in preventing and detecting money laundering and terrorism financing:

1. Provides technical assistance to employees in implementation of measures for detection and prevention of money laundering and financing of terrorism,

2. Provides advice to reporting entity management regarding formulation of the ML/FT risk policy and drafting of internal enactments,

3. Regularly informs the reporting entity management regarding ML/FT activities,

4. Cooperates with other reporting entities of the sector in formulation of the policy for detection and prevention of ML/FT,

5. Ensure proper and timely delivery of data to the APML, pursuant to the Law;

6. Participate in the setting up and development of IT support;

7. Participate in the development of professional education, training and improvement programs for employees of the reporting entity.

The management of a reporting entity and employees must provide to the compliance officers the necessary conditions for work, assistance and support in conduct of their duties, notify them of facts which might be connected with money laundering or terrorism financing, provide unlimited access to information and documents required for the conduct of their duties, adequate HR, material, IT and other conditions for work, adequate premises and technical facilities which ensure protection of confidential information at their disposal, continuous capacity building, replacement during their absence, protection in terms of protection with respect to disclosure of information about them to unauthorized persons.

A reporting entity must set out a cooperation procedure among the compliance officer and other organizational units.

A reporting entity must send to the APML information about the name and position of the compliance officer and deputy compliance officer, and information about the name and position of the member of top management responsible for implementation of the Law, including any changes in such data, within 15 days from the date of appointment.

4. REGULAR PROFESSIONAL EDUCATION, TRAINING AND CAPACITY BUILDING OF EMPLOYEES

Pursuant to provisions of Article 53 of the Law, a reporting entity must ensure regular professional education, trainings and capacity building of all employees performing AMLTF activities, and those who directly or indirectly carry out the activities of detection, prevention of money laundering and terrorism financing, those who perform activities that entail higher risk with respect to money laundering and terrorism financing and of outsourced persons and contracted persons delegated to perform such activities, except when they are independent reporting entities applying measures for detection and prevention of money laundering and terrorism financing, pursuant to Article 4 of the Law.

A reporting entity must ensure that each employee understands their role in the ML/TF risk management process, in order to enable adequate management and control of risks. Therefore, training of employees in direct contact with clients or employees who perform transactions is vital in the ML/TF risk management process. All employees at all levels of seniority to the top management must be aware of the ML/TF risks.

The professional education, training and capacity building include learning about the provisions of the Law, regulations adopted pursuant to the Law, and internal enactments, publications on the prevention and detection of money laundering and terrorism financing, including the list of indicators for identifying customers and transactions in relation to which there are reasons for suspicion of money laundering or terrorism financing.

By March of the current year for the current year, a reporting entity must develop together with the compliance officer an annual program of professional education, trainings and capacity building for employees working on prevention and detection of money laundering and terrorism financing. The program must provide:

1. The contents and scope of the professional development program,

2. The goal of the professional development program,

3. The method for implementation of the professional development program (lectures, workshops, trainings etc.),

4. To whom the program is intended for,

5. The duration of the program.

A reporting entity must also include all new employees in the professional development program. To that end, obligors shall organize a special separate program of

professional education and development for detection and prevention of money laundering and terrorism financing. The program must include at least the provisions on customer due diligence, ML/FT risk assessment, reporting to the Administration for the Prevention of Money Laundering and Terrorism Financing, requirements regarding safety and storage of information and procedures for the implementation of the Law, Regulation of the APML governing methodology for performance of activities in accordance with the Law and the Guidelines and internal bylaws and instructions.

The regular professional education, capacity building and trainings can be implemented by the compliance officer, deputy compliance officer or some other capable professional appointed by the management at the proposal of the compliance officer.

5. REGULAR INTERNAL CONTROL AND INTERNAL AUDIT

Pursuant to Article 54 of the Law, obligors must incorporate regular and systematic internal controls of regularity and efficiency of application of the stipulated measures for the detection and prevention of money laundering and terrorism financing. The purpose of the internal controls is to find and eliminate deficiencies in measures for detection and prevention of money laundering and terrorism financing and to advance the system for detecting transactions or customers with respect to which there are reasons to suspect money laundering and terrorism financing.

Reporting entities should control regularity and efficiency of application of stipulated measures for the detection and prevention of money laundering and terrorism financing by regular or extraordinary supervision, during internal control procedures pursuant to the Regulation of the Administration for the Prevention of Money Laundering governing methodology for performance of activities in accordance with the Law.

A reporting entity must carry out internal control in accordance with the established money laundering and terrorism financing risk. If a reporting entity assessed their risk of operation at a higher level, internal control of operations will be conducted periodically, quarterly or half-yearly, all in accordance with the assessed risk of the reporting entity's operations.

If there is a change in business processes of a reporting entity (e.g. extending/decreasing business activities for which a license has been obtained from the supervisory authority, organizational changes, changes in business procedures, introduction of a new service), a reporting entity is required to check and align the procedures within the internal control, making them compliant with the Law.

A reporting entity is required to review compliance of the systems and procedures with the Law, and their application at least once a year and every time there is a change in the business process of the reporting entity, not later than the day of introduction of such change.

A reporting entity and management bodies of the reporting entity are responsible for the facilitation and organization of internal control in accordance with the Law and the rulebook of the APML governing methodology for performance of activities in accordance with the Law.

A reporting entity provides in an enactment authorizations and responsibilities of the management bodies, organizational units, compliance officers and other entities within the reporting entity how internal control is conducted and its frequency.

A reporting entity is required to prepare an annual report on the conducted internal controls, which shall also state the undertaken steps following the control by 15 March of the current year for the previous year. The annual report contains:

1) The number of reported cash transactions amounting to EUR 15,000 or more in RSD equivalent;

2) The number of reported transactions or persons suspected of a connection with money laundering and terrorism financing;

3) The number of transactions or persons suspected of a connection with money laundering and terrorism financing reported to the Compliance Officer by the reporting entity's employees, but not reported to the APML;

4) The number of established business relations where the customer's identity was established based on a qualified electronic certificate of the customer and the number of business relations established by an empowered representative;

5) Frequency of use of individual indicators for recognizing suspicious transactions when employees report transactions to their Compliance Officer;

6) The number of internal controls executed based on the rulebook and the findings of the internal control (the number of observed and corrected errors and their description etc.);

7) Measures undertaken based on executed internal controls;

8) Information about the executed internal controls of information technologies used in application of the provisions of the Law (ensuring data protection, keeping information about customers and transactions in the centralized data base);

9) Information about the contents of the plan of training on detection and prevention of money laundering and terrorism financing, locations of the trainings and information about

the trainers, number of employees who attended the trainings and an appraisal of future employee training needs;

10) Information about the undertaken measures on data protection which are official secret;

11) The number of established business relations where the third person was delegated to conduct due diligence.

A reporting entity is required to organize an independent internal audit of regular assessment of adequacy, reliability and efficiency of the system for managing ML/TF risk, when the law on operations of the reporting entity requires an independent internal audit, or when the reporting entity assesses that, given the size and nature of its business, there is a need for an independent internal audit under the Law.

The management must ensure that the scope of internal audit is proportionate to the level of ML/TF risk to which the reporting entity is exposed.

A reporting entity must establish the procedure employed at the time of recruitment of candidates for a job involving the application of the provisions of the Law and the regulations passed under the Law. The candidates for such position must be examined in order to establish whether they have been convicted for any of the criminal offenses entailing illegal proceeds or any of the criminal offenses linked to terrorism.

6. INDICATORS FOR SUSPECTING MONEY LAUNDERING AND TERRORISM FINANCING

Pursuant to the Law, reporting entities must develop a set/list of indicators for the identification of persons and transactions with respect to which there are reasons for suspicion of money laundering or terrorism financing (Article 69 of the Law).

When developing a set of indicators, a reporting entity is required to include the indicators published on the APML website, and the indicators the reporting entity has recognized as indicators of money laundering and terrorism financing activities.

When developing a set of indicators for the identification of persons and transactions, suspicious transactions are those which according to their nature, scope, complexity or relatedness are unusual, i.e. without clear economic or legal purpose, or transactions that are disproportionate to the usual or expected business operations of a customer and other circumstances pertaining to the status or other characteristics of the customer.

When establishing if there are reasons for suspicion of money laundering or terrorism financing, the reporting entity must apply the list of indicators and consider other circumstances that indicate the existence of the reasons for suspicion of money laundering or terrorism financing.

7. RECORDS

A reporting entity must keep records on customers, business relations and transactions referred to in Article 8 of the Law.

The content of records on customers, business relations and transactions is laid down in Article 99 of the Law.

8. IMPLEMENTATION OF MEASURES FOR DETECTION AND PREVENTION OF MONEY LAUNDERING AND FINANCING OF TERRORISM IN BRANCHES

Reporting entities must establish a system of measures for detection and prevention of money laundering and financing of terrorism in their branches. To that end, a reporting entity must ensure that the actions and measures for the prevention and detection of money laundering and terrorism financing stipulated by the Law are applied to the same extent in branches and majority-owned subsidiaries which are headquartered in a foreign state, unless stipulated otherwise by the laws of such state (Article 48 of the Law).

A reporting entity must:

- On time and regularly, send to its business units or majority-owned subsidiaries in a foreign country updated information on the procedures concerning the prevention and detection of money laundering and terrorism financing, and particularly concerning customer due diligence actions and measures, reporting to the APML, record keeping, internal control, and other circumstances related to the prevention and detection of money laundering or terrorism financing.

- Determine in its internal enactments the method of conducting control of implementation of the procedures for the prevention of money laundering and terrorism financing at the level of the group.

- Ensure that all business units are acquainted with the policy of implementation of measures for detection and prevention of money laundering and financing of terrorism.

- Ensure that constant supervision is exercised and efficiency of implementation of measures for detection and prevention of money laundering and financing of terrorism ensured in business units.

9. OTHER ACTIVITIES AND MEASURES

Confidentiality of information

A reporting entity must keep as a business secret and treat in accordance with the Law, the information it receives.

All employees and other persons privy to the information must ensure the information remains confidential.

Notwithstanding the above, pursuant to the Law, reporting entities must treat as business secret or confidential information (information that must not be disclosed to customers or third parties) the following:

- Information that there are reasons for suspicion of money laundering or terrorism financing concerning a customer or a transaction and that the information is submitted to the APML,
- Information on suspension of a transaction and the details thereof,
- Information about the APML instruction to monitor financial operations of a customer,
- Information concerning the fact that investigation might be or is initiated concerning a customer or a third person about money laundering and terrorism financing.

The duty of keeping the information confidential shall not apply in circumstances when: The information is required as evidence in the course of law, if the information is required in writing i.e. as instructed by the competent court, or if the information is required by the APML or the Commission enforcing the Law; when information exchange occurs within an international group and when information exchange occurs among reporting entities about the same customer or transaction, providing that the reporting entities are from the Republic of Serbia or a third state that prescribes obligations related to the prevention of money laundering and terrorism financing in accordance with the Law (Article 90).

The access to information classified as confidential or a business secret must be limited. Obligors must internally regulate the conditions and the way the information is accessed, taking into account the following:

1. Information and documentation should be archived in the manner and form preventing unauthorized access (in adequate technical or physically secure archiving premises, locked cabinets and similar),

2. Only members of management and supervisory board of the reporting entity, Compliance Officer and Deputy Compliance Officer, general managers of business units of the reporting entity and other persons authorized by the management have the right to information about customers and transactions with respect to which there are reasons to suspect money laundering and terrorism financing,

3. The documentation with such information shall not be photocopied, written down, edited or published or in any other way reproduced without a prior written authorization by the person responsible,

4. In cases when the documentation is photocopied, a reporting entity must ensure that copies clearly indicate from which documentation or part of the document it has been made, it must be conspicuously indicated that it is a photocopy, the number of photocopies and a signature of the person who has made the photocopies,

5. Employees of a reporting entity must enter passwords when logging in and logging out at the end of data processing and by doing so prevent unauthorized access to documents,

6. A system monitoring data access and processing must be established,

7. Any data transmission shall be allowed only in ways preventing unauthorized access to information either by own courier service or in a sealed envelope via registered mail with postal confirmation and similar, and in cases of electronic delivery a system of safe electronic data transmission should be utilized (data encryption etc.),

8. Employees of a reporting entity must consistently apply the laws governing safety of personal information and the laws governing confidentiality of information.

Data retention

With respect to keeping information, reporting entities must act pursuant to Article 95 of the Law and:

- Information and documentation about a customer, established business relation with the customer or executed transactions, obtained in accordance with the Law, must be kept for at least ten years after the end of the business relation or date of executed transaction.

- Information and documentation about the compliance officer, deputy compliance officer, and employee capacity building and executed internal controls must be kept for at least five years from the day of termination of duty of the compliance officer, conducted capacity building and executed internal controls.

THE LEGAL NATURE AND APPLICATION

The Guidelines are promulgated on the basis of Article 114 of the Law and shall be binding on all reporting entities referred to in Article 110, paragraph 1 of the Law.

The Guidelines shall come into force on the day of their adoption and shall be published on the website of the Securities Commission www.sec.gov.rs.

The Guidelines shall be applied from the day of their adoption, repealing the Guidelines for Application of the Law on Prevention on Money Laundering and Terrorism Financing for Entities Supervised by the Securities Commission, from 9 February 2018.

No: 4/5-112-468/24-18

Belgrade, 8 November 2018

CHAIRMAN

Predrag Dedeić, PhD, Sgd.