MONTENEGRO
SECURITIES AND EXCHANGE COMMISSION

GUIDELINES
for risk analysis aimed at preventing money laundering and terrorism financing for securities market participants

January 2015

Contents

Pursuant to Article 7 paragraph 3 of the Law on Prevention of Money Laundering and Terrorism Financing („Official Gazette of Montenegro“, No. 33/14) and Article 2 paragraph 1 of the Regulation on guidelines for drawing up the analysis and risk factors for prevention of money laundering and terrorism financing („Official Gazette of Montenegro“, br. 53/14), and exercising powers stipulated under Article 94 of the Law on Prevention of Money Laundering and Terrorism Financing („Official Gazette of Montenegro“, No. 33/14), the Securities and Exchange Commission at its 145th session held on 30th of January 2015 has adopted

GUIDELINES
for risk analysis aimed at preventing money laundering and terrorism financing for securities market participants

1. BASIC PROVISIONS

1.1. Competence of the Securities and Exchange Commission

The Securities and Exchange Commission (hereinafter referred to as: the Commission) is authorized, based on Article 7 paragraph 3 of the Law on Prevention of Money Laundering and Terrorism Financing („Official Gazette of Montenegro“, No. 33/14) (hereinafter referred to as: the Law) and Article 2 paragraph 1 of the Regulation on guidelines for drawing up the analysis and risk factors for prevention of money laundering and terrorism financing („Official Gazette of Montenegro “, br. 53/14), to establish guidelines for risk analysis aimed at preventing money laundering and terrorism financing for securities market participants.

Based on Article 94 paragraph 1 item 3 of the Law the Commission carries out supervision over enforcement of the Law and regulations adopted thereunder, in relation to the following securities market participants:

- investment funds management companies and branches of foreign investment funds management companies;
- pensionfunds management companies and branches of foreign pension funds management companies;
- licensed market participants and branches of foreign licensed market participants;
- legal persons licensed by the Commission for carrying out custodial and depository activities, other than banks; and
- stock exchanges and depository and clearing companies.
  (hereinafter referred to as: reporting entities)

1.2. Guidelines objective

The Guidelines aim at uniform application of the provisions of the Law and regulations made thereunder by reporting entities on the securities market, which are subject to supervision of the Commission.

1.3. Content of the Guidelines

Guidelines establish specific criteria for drawing up internal documents on risk analysis related to money laundering and terrorism financing by reporting entities supervised by the Commission, and which relate to:

- a manner of determining possibilities to establish a business relationship with the customer;
- assessment of customers risk rating;
- a manner of determining products and services risk rating, in terms of prevention of money laundering and terrorism financing;
- a manner of customer's identification;
- preventing the use of new technologies for the purpose of money laundering and terrorism financing;
- risk management related to money laundering and terrorism financing to which reporting entities are exposed; and
- employees training program.

Guidelines establish a procedure of including persons in the list of politically exposed persons, in order to implement procedures of enhanced customer due diligence in accordance with the Law, as well as the procedure of termination of obligation to treat persons as politically exposed persons.

Guidelines establish procedure for monitoring transactions and business activities carried out by a politically exposed person, especially bearing in mind the purpose and intended use of a transaction, as well as compliance with its regular business operations.

1.4. Definition of money laundering and terrorism financing

In terms of Article 2 of the Law, the following actions shall be considered money laundering:

- substitution or transfer of funds or other assets in the knowledge that they originate from criminal activities or from participation in those activities, with the aim of concealing or disguise the illicit origin of assets or of assisting any person involved in the commission of criminal offence for the purpose to avoid sanctioning his behavior;
- concealment or disguise of the nature, origin, location, movement, disposal or ownership of money or other assets in the knowledge that they originate from criminal activities or from participation in those activities;

- acquisition, possession or use of assets in the knowledge that, at the moment of the receipt, such assets originate from criminal offence or participation in the same; and
- participation in the commission of criminal offence, conspiracy to commit, attempt to commit and aiding, abetting, facilitating and counseling related to execution of the above mentioned actions.

In terms of Article 3 of the Law the following actions shall be considered terrorism financing:

- providing or collecting, i.e. an attempt of providing or collecting funds, securities, other assets or property, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out an act which constitute an offence;and
- incitement or aiding in providing or collecting funds or assets referred to in the above indent.

The risk of money laundering and terrorism financing is a risk that the customer will misuse the financial system for money laundering or terrorism financing, i.e. that a business relationship, transaction or product will be directly or indirectly used for money laundering or terrorism financing.

1.5. The process and the most frequently used methods of money laundering and terrorism financing

Money laundering process is usually carried out through the following stages:

- Placement stage represents the moment when the assets illegally acquired are separated or moved away from its real - illicit source by different methods and techniques and invested in the financial system for the first time. In this stage"dirty" money is the most visible and exposed to detection;
- Layering stage covers the process when funds are layered in financial flows when, through performing of set of complex transactions, the source of illegally acquired funds or owners of those funds try to be concealed. In this stage, detection of "dirty" money becomes more complicated; and
- Integration stage represents the final stage of money laundering. If legally acquired assets are successfully placed into the financial system and through a layering stage moved away from its illegal source in this stage "dirty" money is included in legal financial flows, by which it is merged with other values of the financial system of the country, which practically enables detection.

Unlike the money laundering process, terrorism financing is not always preceded by an illicit activity, which means that the sources of funding may be legal or illegal. Likewise, the amounts of terrorism financing are not always large, and transactions do not have to be complex as in money laundering. Mentioned circumstances make it difficult to detect terrorism financing

which is why measures used for prevention of money laundering are not sufficient, and must be supplemented by special measures prescribed by the competent international bodies.

Along with technological development the number of sophisticated and complex methods used to disguise the origin of illegally acquired assets has increased. Several most frequently used methods by which the system for detection and prevention of money laundering is attempted to be circumvented are:

- Multiple transactions - if the same person in one day executes two or more transactions, and the total number of transactions in a single day exceeds the prescribed limit for identification or reporting to the Administration for Prevention of Money Laundering and Terrorism Financing;
- Fictitious companies - *shell* companies disguise money laundering assets, and *front* companies carry out legal business activities for concealment of money laundering. This method is often used in layering stage, and money laundering process itself may be also carried out in several countries;
- Casinos - a person walks into a casino with cash and buy chips, plays for a while, and then cashes in the chips taking payment in the check which afterwards deposits into a bank account of third parties;
- Nominees - a person who wants to conceal the origin of illegally acquired assets uses nominees (family members, friends, business associates), who enjoy the confidence of the community, carrying out transactions on their behalf and thus draws attention from illicit activities. This is the most commonly used method of money laundering and concealment;
- Structuring – larger amounts of transactions are structured thus avoiding the obligation to report on cash transactions, changing the amounts of transactions for avoiding identification of a customer, i.e. filling and submission of appropriate documentation required by regulations related to prevention of money laundering. Such amounts of transactions are the most frequently deposited into financial system by larger number of persons;
- Purchasing property with cash - in purchasing luxury goods, real estate and land with cash, the property is usually registered in the name of a close associate or a relative for the purpose to conceal the beneficial owner. The resale of the property is often used to conceal its true origin and a beneficial owner; and
- Redemption of the currency – a foreign currency is bought by illegally acquired funds, which is usually transferred to bank accounts in *off-shore* financial centers.

There are two primary methods used for terrorism financing. The first method involves collection of financial support from countries, organizations or individuals, and the second method involves legal and illegal activities that generate income. When sources of financing of terrorism activities originate from illegal activities, then the approach based on money laundering risk assessment can be also applied to terrorism financing. When sources of

financing of terrorism activities arise from legal activities, it is more difficult to determine whether these funds are used for terrorism purposes.

1.6. Guiding principles on combatting money laundering and terrorism financing

1.6.1. Law enforcement and standard

In performing its registered activities, reporting entities must behave in accordance with laws and regulations that govern detection and prevention of money laundering and terrorism financing and ensure respect for the prescribed measures and activities at all levels, so that the entire reporting entities business operations are carried out in accordance with the Law.

1.6.2. Establishing and verifying the identity of a customer

Before establishing a business relationship or execution of a transaction, a reporting entity must establish and verify the identity of a customer, as well as the identity of a beneficial owner of the customer on the basis of documents, data and information with which undoubtedly and reliably the identity of the customer can be verified.

The identity of the customer can be solely established on the basis of credible, independent and objective sources, like official identification document or other public documents that prove the veracity of customer's identity (personal documents, official documents, original or certified documents from appropriate public register, obtaining data directly from the customer, identifying and verifying the identity of the representative, procurator, proxy of a legal person, establishing and verifying the identity of a natural person by a qualified electronic certificate, based on the statement of the truthfulness of the data collected).

When a customer's identity cannot be established or verified, as well as when it is not possible to identify a beneficial owner of the customer and when it is not possible to obtain information on the purpose and intention of a business relationship or transaction and other data in accordance with the Law, a reporting entity must not establish a business relationship or execute a transaction, i.e. it must terminate any existing business relationship with the customer concerned.

1.6.3. Cooperation with the Commission and the Administration for Prevention of Money Laundering and Terrorism Financing

Within their legal powers, reporting entities must ensure full cooperation with the Commission and the Administration for Prevention of Money Laundering and Terrorism Financing (hereinafter referred to as: the Administration).

The obligation of cooperation of the reporting entity with the Commission and the Administration is particularly important in the case of submission of documents, data and

information related to customers and/or transactions where there are grounds for suspicion of money laundering or terrorism financing.

Cooperation is also needed in the case of reporting on any conduct or circumstances that are, or could be, related to money laundering or terrorism financing which could harm the security, stability and reputation of the financial system of Montenegro.

Therefore, reporting entities' internal procedures in any case may not, directly or indirectly, limit cooperation of reporting entities with the Commission and/or Administration or in any way affect the efficiency of such cooperation.

1.6.4. Establishment of internal policy, procedures and the internal audit

Reporting entities are required to establish a unified policy for risk management related to money laundering and terrorism financing, and based on it, adopt efficient internal procedures, particularly in terms of: customer's identification, risk analysis, identifying customers and transactions for which there are grounds for suspicion of money laundering or terrorism financing .

Risk management policy must include:

- procedures for reception and dealing with customers;
- preparation of risk analysis procedures;
- training employees procedures;
- internal audit mechanisms;
- procedures for identifying and reporting of suspicious transactions; and
- the responsibility of employees to implement measures for detection and prevention of money laundering or terrorism financing.

1.6.5. Regular professional training and education of employees

Reporting entities must provide regular professional training and education of all employees who directly or indirectly carry out activities of prevention or detection of money laundering and terrorism financing, and who carry out activities which are more risky in terms of money laundering or terrorism financing, as well as their authorized persons authorized by a reporting entity to carry out activities of prevention or detection of money laundering and terrorism financing.

2. MEASURES FOR PREVENTION OF MONEY LAUNDERING AND TERRORISM FINANCING

2.1. System for prevention of money laundering and terrorism financing

The Law defines a set of measures and actions which reporting entities are obliged to undertake with the aim to prevent money laundering and terrorism financing, and which presume the obligation of a reporting entity to:

- identify risks and carries out assessment of risk and to undertake actions for money laundering and terrorism financing risk reduction;
- establish the identity of a customer and to perform verification of customer's identity on the basis of credible, independent and objective sources and monitor business operation of a customer;
- deliver information, data and documentation to administration body competent for prevention of money laundering and terrorism financing;
- appoint a person authorized for implementation of measures for detection and prevention of money laundering and terrorism financing and his/her deputy and to provide conditions for their work;
- organize regular professional training and education of employees;
- regularly update the list of indicators for identification of suspicious customers and transactions;
- keep records and to provide protection and safeguard data and documentation obtained in accordance with the Law;
- establish and monitor the system which allows it to fully and timely respond to demands of the competent state bodies in accordance with the Law; and
- implement measures to detect and prevent money laundering and terrorism financing in business units and companies majority-owned by a reporting entity in foreign countries.

Reporting entities should ensure that their system of money laundering and terrorism financing allows application of risk assessment approach, in order to ensure efficient allocation of resources, i.e. greater focus on those areas that represent a higher risk of money laundering and terrorism financing.

For the establishment of an effective system of prevention of money laundering and terrorism financing it is necessary to identify those parts of reporting entities' business operations which are the most exposed to the risk mentioned, as well as to understand the risks to which a reporting entity is exposed due to inefficient system of preventing money laundering and terrorism financing.

2.1.1. Authorized person and his deputy

A reporting entity is required to appoint an authorized person for implementation of measures for detection and prevention of money laundering and terrorism financing (hereinafter referred to as: the authorized person) and his deputy. The above mentioned persons are responsible for

implementation of prescribed measures and actions taken for the prevention of money laundering and terrorism financing.

Requirements for the appointment of an authorized person and his deputy, as well as their duties are stipulated by the Law.

Pursuant to Article 46 of the Law, a reporting entity is obliged to provide to the authorized person and his deputy proper working conditions. In this sense, the reporting entity is obliged to ensure that the authorized person performs its duties as an independent organizational part that is directly responsible to the senior management of the reporting entity.

2.1.2. Professional training and education of employees

Pursuant to the provisions of Article 47 reporting entities are required to provide regular professional training and education of employees who perform tasks related to prevention of money laundering and terrorism financing (hereinafter referred to as: PMLTF).

Reporting entities are required to provide regular professional training and education also for other employees who perform tasks that are, or may be, directly or indirectly, exposed to the risk of money laundering and terrorism financing. In the process of education and training a reporting entity is also required to include all new employees prior to interactions with customers.

Within the education a reporting entity is obliged to inform their employees with the provisions of the Law, regulations adopted thereunder, international standards arising from international conventions in the field of PMLTF, with internal document of the reporting entity, guidelines and the list of indicators for identifying suspicious customers and transactions.

Through training, reporting entities should provide their employees with more clear understanding of their role in the PMLTF system, i.e. understanding of their specific duties and responsibilities.

Reporting entities are required to draw up an annual program of professional training and education in the field of PMLTF for each calendar year within the period prescribed by Law.

Program must include:

- Content and scope of educational program;
- Educational program objectives;
- A manner of realization of educational program (lectures, workshops, practice etc.); and
- A group of employees the educational program is intended for.

The authorized person or his deputy, i.e. another qualified person appointed by reporting entity's management at the proposal of the authorized persons, may conduct training through

internally organized workshops or otherwise provide education of employees about PMLTF (internal portal, online, etc.).

A reporting entity is required to document the period and a manner of training, training content, as well as a list of persons who attended the training. In three days time after the training, a reporting entity should inform the Commission and the Administration about the training.

2.1.3. Internal document

Reporting entities are required to prepare internal documents to analyze the risks of money laundering and terrorism financing in accordance with these Guidelines. Risk analysis should include a risk assessment for each group or type of customer, business relationship, service which a reporting entity provides within the scope of its activity or transaction.

Internal document should establish:

- risk analysis of a customer, business relationship or transaction;
- criteria for identifying unusual transactions;
- the process of implementation of measures of enhanced analysis including measures of permanent monitoring of the business relationship, in accordance with the identified risk;
- a process which determines whether the customer is a politically exposed person;
- a manner for identification and procedures of employees after identification of suspicious transactions and customers;
- responsibility of authorized persons and other employees involved in implementation of the Law;
- a manner of delivery of information and cooperation between the authorized person and employees; and
- record keeping.

By internal document, a reporting entity shall separately prescribe measures taken for the purpose of risk management that accompanies a business relationship or transactions with customers who are not physically present, as well as measures to prevent the use of new technologies for the purpose of money laundering and terrorism financing.

2.1.4. The list of indicators for identifying suspicious customers and transactions

The List of indicators established by the Ministry of Finance presents the basic guidelines for identifying suspicious circumstances associated with a specific customer, transaction or business relationship, and it is therefore necessary to ensure that reporting entity's employees are familiar with indicators in order to apply them in their work efficiently.

Reporting entities are required to include the list of indicators for the secutities market in their internal document for risk analysis, which they may amend and adapt according to trends and typologies of money laundering known to them, as well as circumstances arising out of their business operations.

2.1.5. Internal audit

Article 48 of the Law stipulates the obligation of a reporting entity to ensure regular internal control and audit of implementation of programs for prevention of money laundering and terrorism financing, i.e. performance of activities related to detection and prevention of money laundering and terrorism financing.

In their operations, reporting entities shall abide by the Regulation on the work of the authorized person, a manner of exercising internal control, record keeping and safeguarding of data, a manner of record keeping and training of employees ("Official Gazette of Montenegro" No. 48/14 of 13/11/2014), which was adopted by the Ministry of Finance, and which specifies in more detail acting upon requests referred to in Article 48 of the Law.

The objective of internal audit is to determine and eliminate shortcomings in implementation of the prescribed measures for detection and prevention of money laundering and terrorism financing, as well as improving the system for detection of suspicious customers and transactions.

2.1.6. Record keeping

Types and contents of records which a reporting entity is obliged to keep are prescribed under Article 78 and Article 79 of the Law.

2.1.7. Establishment of an adequate information system

Reporting entities are required to establish an adequate information system in order to, at the request of the Administration and other competent authorities, fully and timely deliver information on how they maintain or maintained a business relationship with a particular natural or legal person and what is the nature of this relationship.

Established information system would, in addition to the above mentioned, allow the authorized person and his deputy a permanent and safe monitoring of activities in the field of PMLTF.

For this purpose, reporting entities should establish an information system that will allow keeping records on customers for whom an enhanced analysis was carried out and other records prescribed by the Law, as well as simple and efficient search of all the information collected about customers, transactions and business relationships. Such system should also allow the effective monitoring of business relationships and easier identification of suspicious transactions.

Article 6, paragraph 1, item 8 of the Law stipulates the obligation of a reporting entity to establish a system that allows full and timely response to the requirements of administration bodies and the competent state authorities in accordance with the Law.

2.2. Risk assessment

The approach based on risk assessment enables a reporting entity to focus on areas with greatest risk and, on the other hand, reduction of requirements in areas where the risk is low.

The reporting entity is required to regularly update all procedures and techniques upon which the analyzes was made and manage the risks of money laundering and the terrorism financing.

2.2.1. Risk analysis

In the process of risk analysis, taking into account the nature, scope and complexity of its business operations, a reporting entity shall define:

- assessment of the likelihood that its business operations can be misused for money laundering or terrorism financing;
- criteria and risk factors based on which it shall classify a certain customer, business relationship, product or transaction in a particular category of risk of money laundering or terrorism financing;
- consequences and measures for the efficient management of such risks.

2.2.2. Evaluation of risk rating

Evaluation of customer's risk rating, business relationships, products or transactions of money laundering or terrorism financing involves their classification into a certain risk category. In so doing:

- a reporting entity may classify, in accordance with its risk management policy, a particular customer, business relationship, product or transaction in the high risk category;
- a reporting entity may not itself expand the group of customers, business relationships, products or transactions, which will be classified into a low risk category;
- a reporting entity must not classify customers, business relationships, products or transactions that have been, by the Law and regulations adopted thereunder and these Guidelines, defined as high risk, into the category of medium or low risk;
- a reporting entity should adequately document and regularly update any evaluation of customer's risk rating, business relationships, products or transactions of money laundering or terrorism financing.

2.2.2.1. Initial assessment and reassessment of risk

Based on risk analysis conducted, a reporting entity must prepare evaluation of risk rating of a certain customer, business relationship, product or transaction (before establishmentof the business relationship or execution of transaction), and after implementation of the following stages:

- establishment of the identity of a customer with the collected required data about the customer, business relationship, product or transaction and other information, that should be collected by a reporting entity for evaluation of risk rating;
- evaluation of data collected in connection with the criteria and risk factors of money laundering or terrorism financing (risk identification); and
- specific forms of verification and monitoring of customer's business operations (enhanced and simplified due diligence).

Within the framework of measures for regular monitoring of the business relationship with the customer, a reporting entity re-evaluates the groundedness of the initial risk rating or a business relationship, and if it proves necessary, a reporting entity determines a new risk rating. The reporting entity subsequently re-evaluates the groundedness of the initial risk rating of a particular customer or a business relationship in the following cases:

- if circumstances on which risk rating of a particular customer or business relationship have significantly changed, as well as its classification into a specific category of risks; and
- if a reporting entity has doubts about the authenticity of information based on which it determined risk rating of a particular customer or a business relationship.

2.2.2.2. Evaluation of risk rating

When determining risk rating of a particular customer, business relationship, product or transaction, a reporting entity should take into account the following criteria:

- type, business profile and ownership structure of the customer;
- geographical origin of a customer;
- the nature of a business relationship, product or transaction;
- past experience of a reporting entity with a customer;
- presence of a customer at the conclusion of a business relationship or transaction execution, especially taking into account the use of new technologies enabling anonymity (e.g. online banking); and
- other information showing that a customer, a business relationship, product or transaction may be riskier.

2.2.2.3. Risk categories

Starting from risk factors and being led by the risk criteria, reporting entities are obliged to classify customers, business relationship, product and transaction into three main risk categories:

a) high risk;
b) medium risk; and
c) low risk.

a) High risk

Customers who fit into the category of high risk are:

1) customers whose source of funds is unknown or unclear, i.e. which the customer cannot prove;
2) customers who are suspected of not acting for its own account, i.e. that carry out the instructions of a third party;
3) customers that carry out business activity or execute transaction under unusual circumstances, especially taking into account its grounds, the amount and manner of execution, purpose and the like or by which is meant:
    - substantial and unexpected geographical distance between customer's location and organizational unit of a reporting entity where the customer establishes a business relationship or executes a transaction;
    - frequent and unexpected establishment, without economic justification, of similar types of business relationships with more securities market participants, such as opening accounts with several securities market participants, conclusion of several agreements on mediation in a shorter period of time, etc.;
    - frequent transfers of funds from one fund to another;
    - cancellation of membership immediately after conclusion of the contract of membership in the fund;
    - a requirement that the funds accumulated in the individual account of a fund member are paid to the account of a third party or to the account of a person in the territory of a country which does not apply strict standards in the area of money laundering and terrorism financing;
    - Insistence on secrecy of transactions and the like.
4) customers where, because of the structure, legal form or complex and ambiguous relations, it is difficult to determine the identity of their beneficial owners, such as off-shore legal persons with unclear ownership structure and which were not established by a company from the country which applies the standards in the area of money laundering and terrorism financing that comply with the standards prescribed by the Law;
5) customers who carry out activities characterized by large turnover and cash payments (e.g. carriers of goods and passengers);
6) foreign arms dealers and arms manufacturers;
7) customers represented by persons who professionally carry out this activity (lawyers, accountants or other professional representatives), especially when the reporting entity is in contact solely with the representatives;
8) sports associations;
9) construction companies;
10) companies with a disproportionately small number of employees in relation to scope of work they perform, which do not have their own infrastructure, business premises and the like;
11) customers (natural or legal persons) who are on list of persons subject to measures imposed by the United Nations or the Council of Europe;

12) customers residing or established in entities that are not subject to international law, i.e. that are not internationally recognized as states (such entities give the possibility of a fictitious legal person registration, allow the issuance of fictitious identification documents, etc.);
13) customers whose offer to establish a business relationship was refused by other reporting entity by the Law, regardless of the way this fact became known, i.e. a person who has a bad reputation;
14) a customer who is a politically exposed person in terms of Article 32 of the Law;
15) a customer who is a foreign legal person that does not carry out or is prohibited from carrying out commercial, manufacturing or other activities in the country in which it is registered (a legal person established in the country which is known as an offshore financial center, and which has been imposed certain restrictions for immediate performance of the registered activity in that country);
16) a customer who is a fiduciary or other similar foreign law company with unknown or hidden owners or management;
17) a customer who has a complex ownership structure or complex chain of ownership (complex ownership structure or complex chain of ownership which makes it difficult or prevents identification of a beneficial owner of the customer, or the person who indirectly provides property assets, based on which it has the ability to supervise, and that can be directed or otherwise significantly affect managerial decisions when deciding on funding and business operations);
18) a customer that does not have or is not required to have a license of an adequate supervisory authority to perform its activities, i.e. in accordance with the legislation of the home country is not the subject of measures in the area of money laundering and terrorism financing;
19) a customer who is a non-profit organization (institution, organization or other legal person, i.e. entity that does not carry out business activities) and meet one of the following conditions:
    - has registered office in the country known as off shore financial center;
    - has registered office in the country known as financial, i.e. tax haven;
    - has registered office in the country which is not a signatory of the Treaty on European Union;
    - among its members or founders there is a natural or legal person who is a resident of any of the above mentioned countries;
20) a customer who is a foreign legal person, established by the issuance of bearer securities.

Business relationships, transactions or products that fit into the category of high risk are:

1) transactions which significantly differ from the standard way of execution the transaction;
2) transactions that have no economic justification (e.g. frequent securities trading when the trade is made by depositing cash at the special-purpose accounts and soon after securities are being sold below the price - so-called trading securities at a loss);
3) transactions executed in a way to avoid standard and usual control methods;

4) transactions which include more participants without clear economic reasons, several interconnected transactions executed in a shorter period or in more consecutive intervals, in the amount that is below the limit for reporting to the Administration;
5) loans to legal persons and, in particular, loans from foreign founders to a legal person in the country;
6) transactions where the customer obviously hides the real grounds and the reason for execution of the transaction;
7) payment for services for which there is no determinable value or price;
8) transactions where the customer refuses to provide documentation;
9) transactions where the documentation does not match the manner of execution of a transaction itself;
10) transactions where the source of funds is unclear or where their relationship with customer's business operations cannot be determined;
11) products or transactions that might favor anonymity, such as the use of custody services;
12) announced block trade, especially when newly founded companies or companies registered in offshore destinations appear as buyers;
13) securities trading on the regulated market which were pledged under the loans granted to securities owners;
14) transactions of payment of services to customer's partners that come from off-shore areas, and from records it can be seen that the funds originate from countries in the region;
15) transactions that were intended for persons against whom the measures of the United Nations or the Council of Europe have been imposed;
16) transactions that a customer would execute on behalf and for the account of a person against whom the measures of the United Nations or the Council of Europe have been imposed;
17) transactions where the payment of funds is made from the customer's account, i.e. payment of cash funds to the customer's account different from the account that the customer stated during identification, i.e. through which it usually operates or has operated (particularly in the case of a transaction abroad);
18) payments received from a third party not associated with the payment;
19) transactions intended for persons residing or established in the country known as a financial or tax haven;
20) transactions intended for persons residing or established in the country which is known as an offshore financial center;
21) transactions intended for non-profit organizations established in the country known as offshore financial center;
22) business relationships which include regular or large payments of cash funds from or/and to the customer's account opened with a credit or a financial institution of the country which is not a member of the European Union, i.e. business relationships which, on its own behalf and for the customer's account, a foreign credit or other fiduciary institution established in the country which is not a member of the European Union, concludes in the capacity of a proxy;

23) business relationships entered into at a reporting entity without the personal presence of the customer and in connection with which the conditions for implementation of simplified customer's verification have not been met; and
24) new products and new businesses, including new delivery mechanisms, and the use of new development technologies for both new and old products.

Countries or geographical areas that fit into the category of high risk are:

1) the country against which the United Nations, the Council of Europe or other credible international organizations have imposed sanctions, embargoes or similar measures;
2) countries designated by the Financial Action Task Force (hereinafter referred to as: FATF) or other credible international organization, as countries which finance or support terrorism activities, as well as those which have certain terrorist organizations acting within the same;
3) countries designated by FATF or other credible international organization as countries which do not apply adequate measures for prevention of money laundering and terrorism financing;
4) countries designated by FATF or other credible international organization as countries missing internationally recognized standard for prevention and detection of money laundering and terrorism financing;
5) countries that are, based on estimates of credible international organizations, designated as countries with a high degree of organized crime due to human, firearms and drugs trafficking and other criminal activities;
6) countries where, based on estimates of credible international organizations, high level of corruption and human rights violations has been established;
7) countries which are, by the assessment of international organizations (FATF, the Council of Europe, etc.) classified among non-cooperative countries and territories; and
8) countries which represent offshore areas.

Information on high-risk countries may be obtained on the MONEYVAL website: http://www.coe.int/t/dghl/monitoring/moneyval/, and FATF website: http://www.fatf-gafi.org/.

Reporting entities should consider the following international organizations as the competent international organizations for monitoring the effectiveness of implementation of measures in the area of money laundering and terrorism financing with the provisions of international standards:

- The European Central Bank;
- The EC Committee for the Prevention of Money Laundering and Terrorism Financing;
- FATF;
- The International Monetary Fund;
- The World Bank;
- The International Association of Financial Supervisory Bodies Dealing With Detection and Prevention of Money Laundering and TerrorismFinancing - Financial Intelligence Group (Egmont Group);

- The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL);
- The International Organization of Securities Commissions (IOSCO);
- The European Securities and Markets Authority (ESMA);
- The European Insurance and Occupational Pensions Authority (EIOPA);
- The International Association of Insurance Supervisors (IAIS); and
- The European Banking Authority (EBA).

b) Medium risk

A reporting entity shall classify in the medium-risk category the customer, business relationship, product or transaction that, based on the criteria laid down in the Guidelines and risk factors cannot be classified into the category of high or low risk.

c) Low risk

Customers who fit into the category of low risk are:

1) a reporting entity referred to in Article 4 paragraph 2 items 1, 2, 4, 5, 6, 9 and 11 of the Law or other appropriate institution established in the European Union or a country listed among countries that apply international standards from the field of money laundering and terrorism financing which are on the level of European Union standards or even higher;
2) state authority or local self-government body and other legal entity which exercises public authority;
3) a business organization whose securities are admitted to trading on a regulated market or a stock exchange in EU countries or other countries where international standards which are on the level of European Union standards or even higher are applied;
4) a business organization or other form of performing business activity that exercises public authority and is listed on the stock exchange and subject to obligation to submit information according to the rules of the stock exchange or in accordance with regulations which introduce the obligation of transparency of the beneficial owner of that organization;
5) from the geographical area which falls within less risky areas.

Business relationships, transactions or products that fit into the category of low risk are:

1) life insurance policy where premiums are low;
2) savings in pension plans if there is no possibility of early withdrawal of savings and when savings cannot serve as a collateral;
3) pensions and other plans that provide pension income, in cases in which contributions are provided by subtracting from earnings and whose rules do not allow transfer of members' yields;
4) financial products and institutions that provide specific and limited services to particular type of clients, in order to improve access to financial inclusion;

5) products in which the risk of money laundering and terrorism financing depends on other factors, such as limitations on the amount of electronic money and transparency of ownership.

Countries or geographical areas that fit into the category of low risk are:

1) countries that are members of the European Union;
2) countries that have an efficient system of combating money laundering and terrorism financing, identified by FATF;
3) countries where a low level of corruption and other criminal activities is determined;
4) countries that implement FATF recommendations to combat money laundering and terrorism financing, and for which verification of compliance with these recommendations is carried out.

2.3. Establishment of customer's identity and specific forms of verification and monitoring of customer's business operations

A reporting entity shall establish and verify the identity of a customer (natural person/legal person), its agent, a beneficial owner of the customer (for legal persons) and other persons authorized by the customer to represent him before a reporting entity, in the manner stipulated by the Law.

A reporting entity is obliged to implement measures for identification and verification of the identity of a customer and monitoring customer's business operations prescribed in Article 8 of the Law in all cases stipulated by the Law.

2.3.1. Establishing the identity of the beneficial owner

A definition of a beneficial owner is defined under Article 20 of the Law, and a manner of identification of a beneficial owner is stipulated by Article 21 of the Law.

2.3.2. Specific forms of due diligence and monitoring of customer's business operations

Pursuant to Article 29 of the Law, there are specific forms of verification and monitoring of customer's business operations, as follows:

a) Enhanced due diligence and monitoring of customer's business operations; and
b) Simplified due diligence and monitoring of customer business operations.

a) Enhanced due diligence and monitoring of customer's business operations

Article 30 of the Law sets out the conditions in which a reporting entity is obliged to carry out an enhanced customer due diligence and monitoring of customer's business operations. Measures of enhanced due diligence and monitoring of customer's business operations are carried out also in all other cases where a reporting entity assess that, due to the nature of a business relationship, form and manner of execution of a transaction, business profile of a customer or other circumstances related to customer or there could be a high risk of money laundering or terrorism financing.

A reporting entity is obliged, in all cases of high risk of money laundering and terrorism financing, to implement measures of enhanced due diligence and monitoring of customer's business operations, and especially if the customer or a beneficial owner of the customer is a politically exposed person.

Politically exposed person

A definition of a politically exposed person is set forth under Article 32 of the Law, while Article 33 of the Law prescribes measures of enhanced due diligence and monitoring of business operations of politically exposed persons.

Before establishing a business relationship with a customer who is a politically exposed person or a customer whose beneficial owner is a politically exposed person, a reporting entity's employees are required to obtain the written consent of a senior management, and if the business relationship has already been established, it is necessary to obtain the written consent of a senior management for continuance of business relations.

In order to identify politically exposed persons,reporting entities are required to:

- demand from clients to fill in the form for politically exposed persons;
- collect information from public sources;
- collect information on the basis of a review of the database containing a list of politically exposed persons (e.g. the list of politically exposed persons on the website of the Administration, World Check PEP List, etc.);
- collect information on the basis of a review of the database held by the Commission for the prevention of conflict of interest.

In the event that, when completing the form for politically exposed persons, the customer does not declare himself as a politically exposed person, a reporting entity shall, based on the above methods, verify whether the customer is a politically exposed person, and if it turns out that he is, a reporting entity shall take measures of enhanced due diligence and monitoring of business operations.

After establishing a business relationship with a politically exposed person, a reporting entity is also obliged to keep separate records of these persons and transactions concluded on behalf and for the account of such persons, in electronic form.

After obtaining approval from a senior manager for establishment or continuation of a business relationship with a politically exposed person, employed with a reporting entity are not required to obtain approval from a senior manager for undertaking each individual executed for politically exposed persons. However, reporting entity's employees are required to pay special attention to transactions and other business activities carried out by a politically exposed person, and, if necessary, notify the authorized person on these transactions in the shortest possible time.

b) Simplified due diligence and monitoring of customer business operations

Article 37 of the Law sets out cases in which a reporting entity can execute measures of simplified due diligence and monitoring of customer's business operations. The above cases relate to customers, business relationships, transactions or products for which a reporting entity established to belong to low risk category.

When conducting a simplified customers due diligence, a reporting entity must collect and verify information in a manner determined by Article 38 of the Law.

2.4. Supervision over customer's accounts and transactions, measures and frequency of monitoring the business activities of a customer

A reporting entity is obliged to continuously supervise customer's accounts and transactions to prevent money laundering and terrorism financing. A reporting entity can effectively control and reduce the risk only if there is information about the customer's business operations, in order to identify transaction in accordance with the customer's profile. In this sense, a reporting entity is required to establish adequate procedures for regular and careful monitoring of the customer's business activities. A reporting entity should pay particular attention to all complex, unusual large transactions and all unusual customer's activities which have no apparent economic purpose. The subject of intense monitoring are the accounts and transactions associated with customers who are classified into the high risk category for which a reporting entity defines key indicators, such as the origin of funds, type of activity, place of business, etc.

Supervision over customer's accounts and transactions depending on the category of risk**:**

- high-risk category – at least quarterly;
- medium-risk category – at least twice a year; and
- low-risk category – at least once a year.

Reporting entities are required to actively monitor transactions of a customer executed during a business relationship for the purpose to verify whether transactions match the knowledge of a reporting entity on that customer, type of work, source of funds, the purpose and intended nature of a business relationship or transactions.

According to Article 27 of the Law, measures of monitoring business activities particularly include:

- verification of compliance of customer's business operation with the nature and purpose of the contractual relationship;
- monitoring and verification of customer's compliance with its usual scope of business;
- monitoring and regular updating of documents and customer's data, which include performing of repeated annual control of the customer in the cases referred to in Article 28 of the Law.

The purpose of monitoring business activities of a customer is verification of compliance of the customer with the anticipated nature and purpose of the business relationship that the customer established with a reporting entity (established during implementation of measures for identification and verification of the customer's identity and monitoring of customer's business operation) as well as the usual scope of customer's business.

In addition, reporting entities are required to ensure that the volume, i.e. frequency of implementation of measures for monitoring business relationship, are adapted to risk of money laundering or terrorism financing they are exposed to during performance of a particular work, i.e. when dealing with individual customer (also taking into account customer's risk rating, i.e. risk category to which it is classified), and in accordance with Articles 27 and 28 of the Law.

In addition to measures for monitoring a business relationship, reporting entities are required to regularly (at least annually), i.e. at the latest after the expiry of one year from the last control of the customer, carry out repeated annual control of a foreign legal person.

Articles 27 and 28 of the Law stipulate the content, frequency and manner of implementation of measures for monitoring business activities of a customer and repeated annual controls.

The intensity of monitoring business activities of a customer depends on risk rating of a particular customer, i.e. a category of risks to which the customer is classified.

Reporting entities are required to define and regulate procedures for implementation of measures for permanent monitoring of a business relationship by their internal document. By its internal document a reporting entity may prescribe undertaking of additional measures for monitoring business activities of certain customers.

2.5. Managing risks related to money laundering and terrorism financing

A reporting entity is obliged to continuously manage the risks of money laundering and terrorism financing to which it is exposed in its business operations. In this sense, a reporting entity is required to determine those areas of business which are, considering the possibility of money laundering and terrorism financing, more or less vulnerable, i.e. to identify and determine main risks in those areas and measures for solving them.

The system for management of risk related to money laundering and terrorism financing shall include, at least:

- developed processes for risk management;
- clearly defined authorizations and responsibility for risk management;
- efficient and reliable system of information technology;
- a manner and dynamics of reporting and informing the reporting entity's management on risk management.

The system for management of risk related to money laundering and terrorism financing shall provide:

- risk identification;
- risk assessment;
- monitoring and analyzing of risk;
- risk control;
- undertaking of measures and risk minimizing; and
- reporting to the competent authorities.

2.6. Reporting to the Administration and application of the Law and regulations

Obligation and manner of notifying the Administration of suspicious transactions are regulated by the Law and regulations adopted thereunder.

In its business operations, a reporting entity is required to comply with the Law and regulations adopted thereunder, which include:

- Regulation on indicators for identification of suspicious customers and transactions ("Official Gazette of Montenegro", No. 50/14 of 28/11/2014);
- Regulation on a manner of work of the authorized person, a manner of exercising internal control, data keeping and safeguarding, record keeping and training of employees ("Official Gazette of Montenegro", No. 48/14 of 13/11/2014);
- Regulation on guidelines for drawing up the analysis and risk factors for prevention of money laundering and terrorism financing ("Official Gazette of Montenegro", No. 53/14 of 19/12/2014);
- Regulation on conditions and a manner of delivery of data on cash transactions in the amount of at least EUR 15,000 and suspicious transactions("Official Gazette of Montenegro", No. 49/14 of 20/11/2014); and
- Guidelines of the Commission.

3. FINAL PROVISIONS

Reporting entities are required to draw up/comply internal documents for the analysis of risk of money laundering and terrorism financing with these Guidelines and to conduct other activities necessary to ensure their application within the period of 60 days following the date of entry into force of these Guidelines.

On the date of entry into force of these Guidelines, the Guidelines for risk analysis aimed at preventing money laundering and terrorist financing for capital market participants of 9 February 2012 shall cease to be valid.

These Guidelines shall enter into force on 1st of February 2015, and shall be published on the Commission's website.

Number: 01/1-121/1-15
Podgorica, 30th of January 2015

CHAIRMAN OF THE COMMISSION
Zoran Đikanović PhD