CONTENTS

Pursuant to the Law on Prevention of Money Laundering and Terrorist Financing ("Official Gazette of Montenegro", Nos. 033/14 of 4 August 2014, 044/18 of 6 July 2018, 073/19 of 27 December 2019), Guidelines on the risk-based approach and development of risk analysis of money laundering and terrorist financing for the capital market participants, which was adopted by the Capital Market Commission at its 81st session of 31 October 2019 and the Articles of Association of the Investment Company SASA CAPITAL AD Podgorica (hereinafter referred to as: "the Company"), Board of Directors of the Company, on 10 January 2020 has adopted the following:

POLICY AND PROCEDURES FOR RISK ANALYSIS OF MONEY LAUNDERING AND TERRORIST FINANCING

INTRODUCTION

The Guidelines of the Capital Market Commission of 31 October 2019 have been developed to enable the uniform application of the provisions of the Law on Prevention of Money Laundering and Terrorist Financing (hereinafter referred to as: "the Law"), and the regulations adopted by the capital market reporting entities subject of the Commission's supervision.

A risk-based approach and the development of risk analysis of money laundering and terrorist financing is an effective tool for combating money laundering and terrorist financing.

Regular assessment of the money laundering and terrorist financing risk is enabling us to protect and preserve the integrity of our business.

A risk-based approach helps the Company to make a list of its own risks related to products, services and distribution channels, customers and business relationships, geographical and other relevant factors, all in order to implement effective measures aimed at mitigating and monitoring money laundering and terrorist financing risks which the Company may encounter as a part of its activities.

DEFINITION OF RISK

Risk is defined as the likehood of an event and its consequences, or a combination of the chance that something may happen and the degree of damage or loss that may result from such an occurrence. Company-level risk entails threats and vulnerabilities that put it at risk of being used to facilitate money laundering and terrorist financing.

Risk Management

Risk management is a process that includes the recognition of money laundering and terrorist financing risks, risk assessment and the development and application of methods to manage and mitigate the risks that have been identified.

Inherent and residual risks

When assessing risk, it is important to distinguish between inherent and residual risk.

Inherent risk is the intrinsic risk of an event or circumstance that exists before the application of control mechanisms or mitigation measures.

Residual risk is the level of risk that remains after the implementation of control mechanisms and mitigation measures.

Definition of a risk-based approach

A risk-based approach is a process that encompasses the following:

- Risk assessment of the Company's business activities and clients using prescribed criteria/factors, such as:

- Products, services and distribution channels;
- Geography;
- Clients and business relationships, and
- Other relevant factors.

- Mitigation of risk through the implementation of controls and measures tailored to identified risks;
- Updating data on client identification (beneficial owner and business relation information in accordance with assessed level of risk);
- Regular monitoring of transactions and business relationships in accordance with the assessed level of risk.

It is important to emphasize that the assessing and mitigating the mitigation of money laundering and terrorist financing risks has a dynamic properties, which means that the risk that have been identified may change or evolve over time due to the emergence of new products or new threats in the course of the Company's business activities. In the light of the above, the risk-based approach should be re-evaluated and updated when risk factors change.

COMPLIANCE WITH THE LAW

The Company's compliance with the Law implies that the Company:

- Appoints a compliance officer for the identification and prevention of money laundering and terrorist financing;
- Develops and implements compliance policies and procedures;
- Assesses and documents the risks related to money laundering and terrorist financing, as well as to document and implement mitigation measures to mitigate the identified risks;
- Has a regular training program for employees, representatives or other persons authorized to represent (training program shall be made in writing, and training data shall be documented);
- Regular internal control and review of the implementation of programs for the prevention of money laundering and terrorist financing and other policies and procedures with the objective of attesting their effectiveness.

The risk assessment allows for the establishment of procedures and controls that help detect and mitigate possible money laundering and terrorist financing activities.

Conducting high-risk activities or having high-risk business relationships is not contrary to the law. Defining clients as high-risk is an assessment that allows us to undertake controls and measures to mitigate the risks and apply special measures prescribed by the law in such cases.

RISK-BASED APPROACH CYCLE

Risk-based approach entails the following stages:

1. Identification of inherent risk;
2. Creation of the key control mechanisms and risk mitigation measures;
3. Assessment of residual risks;
4. Implementation of the risk-based approach;
5. Verification of the risk-based approach.

FIRST STEP: IDENTIFICATION OF INHERENT RISK

Inherent risk assessment is divided in two parts:

1. Business-based risk assessment entails the review of products offered to the clients, services and distribution channels, geographic location of the business and other relevant factors;
2. Relationship-based risk assessment entails the review of products and services used by our clients, geographic location of our clients, as well as their activities, transaction patterns and methods, etc.

1. Risk-based approach

Identification of inherent risks of business is contingent upon the review of our vulnerability to money laundering and terrorist financing.

The following three elements of risk assessment that are important for business risk analysis are as follows:

a) Products, services and distribution channels;
b) Geography, and
c) Other relevant factors.

a) Products, services and distribution channels

The Company's activities, among other financial instruments, include financial contracts for differences.

Contract for differences (CFDs) are complex financial instruments that carry a large amount of risk, and they are not suitable for investors who do not have the appropriate level of financial knowledge and experience. These derivative financial instruments represent a bilateral agreement between two contracting parties that contain and are contingent upon the fixed assets contained in the derivative.

When trading with CFDs, the transactions are not executed on a recognized or designated stock exchange, but rather on outside organized market[1] (OTC transactions). OTC transactions may involve a higher investment risk because there is no stock exchange on which to close an open position. All positions entered into with the Company must be closed with it and cannot be closed with any other entity. There is neither central clearing system nor guarantee by any other party regarding payment obligations to the Company's client.

Leverage trading, i.e. CFDs trading takes place via telephone and the online trading platform *MetaTrader 5* via the Internet. Since the Company records all conversations with its clients and keeps records of all e-mails, they are subject to examination and control with the objective of preventing money laundering and terrorist financing. Furthermore, the online trading platform contains a record of all transactions and trades conducted through the trading platform.

Prior commencing a business transaction, the client signs a statement that he will comply with all applicable laws and other regulations governing the prevention of money laundering, terrorist financing, illegal business or any other type of financial crime.

Where the client refuses to provide, either at the stage of opening an account or at a later stage, all the necessary information in order to prevent the risk of preventing money laundering and terrorist financing, the Company has the right

[1] OTC or "over-the-counter market" is, in addition to stock exchanges, the second major part of the secondary financial market. This market is not a physical place of trade. This market usually means all purchase and sale activities with securities that do not take place on stock exchanges.

to: terminate the contract with the client, refuse to execute the order and freeze or blocks the client's account, as well as all funds held on the account, develop a report or to notify competent state authorities and submit all information, in accordance with applicable laws governing this area.

b) Geography

The geographical location of the Company's place of business in relation to the countries to which we transfer funds and the countries from which we receive funds provides indications as to whether there are constitutive elements of money laundering and terrorist financing. This applies to the immediate environment, within Montenegro, rural or urban areas, as well as to other countries.

Increased risk of money laundering and terrorist financing is expressed with the clients from certain destinations, and these are in particular the following:

- Countries subject to United Nations sanctions, embargoes or similar measures;
- Countries designated as financing or supporting terrorist activities, as well as the countries having certain terrorist organizations operating in them;
- Countries identified by the Financial Action Task Force (FATF) or other reference international organizations as countries that lack an internationally recognized standard for the prevention and detection of money laundering and terrorist financing;
- Countries that, based on the assessment of the competent international organizations, have been identified as the ones with the prevalence of organized crime due to corruption, arms trafficking, trafficking in white slaves or human rights violations;
- Counties that, according to the international organization (FATF, United Nations Security Council, etc.) have been classified as non-cooperative jurisdictions;
- Countries representing offshore areas.

Client identification

Prior to establishing a business relationship, it is mandatory to conduct the following client identification:

- establishing the identity of the client, or if the identity has been previously established, verifying the identity on the basis of credible, independent and objective sources;
- collecting the data on the client, or if the data are collected, verification of the collected data on the basis of credible, independent and objective sources.

Establishing and verifying the identity of a natural person or entrepreneur

An employee of the Company, who establishes a business relationship with a client, shall establish and verify the identity of a client who is a natural person, or his legal representative, entrepreneur, or a natural person performing an activity, by checking the client's personal identification document issued by the competent state authority (based on which his identity can be undoubtedly be established) in his presence and shall collect the following information:

(a) first and last name, date and place of birth, permanent or temporary residence;
(b) number of the personal identification document and the place of issue, type and name of the authority that issued the personal identification document and the unique citizen's identification number of the natural person opening the account, establishing a business relationship or executing a transaction;
(c) first and last name, date and place of birth, permanent residence, identification document number and place of issue, unique citizen's identification number of authorized person who is opening an account on behalf of another person, establishing a business relationship or executing a transaction;

(d) date of opening the account or establishing the business relationship;
(e) type and purpose of the transaction;
(f) date and time of the transaction;
(g) amount of the transaction;
(h) manner of executing the transaction.

Establishing and verifying the identity of a legal person

An employee of the Company, who establishes a business relationship with a client, shall establish and verify the identity of a client that is a legal person or its legal representative, or an authorized person, by checking the original or certified copy of the document (which must not be older than three months) from the Central Registry of Commercial Entities of Montenegro (hereinafter referred to as: the CRCE) or other appropriate public register, submitted by the representative on behalf of the legal person.

Establishing and checking the identity of a legal person and obtaining data can also be done by checking the CRCE or other appropriate public register. In this case, the register extract shall contain the date, time and personal name of the person that has made the check. The register extract shall be kept in a file with other client documentation.

If data set forth in the Law cannot be obtained by checking the original or certified copies of documents, the missing data shall be obtained directly from the representative or authorized person.

If the employee who establishes and checks the identity of the legal person doubts the accuracy of the obtained data or veracity of documents and other business files from which the data have been obtained, he shall be obliged to obtain from the representative or authorized person a written statement before establishing a business relationship or executing a transaction.

If a client is a foreign legal person performing activities in Montenegro through its business unit, it shall be mandatory to establish and verify the identity of that foreign legal person and its business unit.

Identification of the client – legal person includes:

(a) company, seat, address, unique registration number, tax identification number (hereinafter referred to as: the PIB) of the legal person opening an account, establishing a business relationship or executing a transaction, or on behalf of which an account is being opened, business relationship established or transaction executed;
(b) date of the opening of the account or the establishment of the business relationship;
(c) type and purpose of the transaction;
(d) date and time of the transaction;
(e) amount of the transaction;
(f) manner of executing the transaction.

When establishing identification of the client, the following actions shall be also carried out:

(a) prior to establishing a business relationship or executing a transaction, the identity of the client, as well as the identity of the beneficial owner shall be established and verified on the basis of documents, data and information by which the identity can be established in an unequivocal and reliable manner;
(b) measures shall be taken to verify and establish the client's ownership structure and actual control of the client in order to establish the identity of the beneficial owner of the client;

(c) data and documentation shall be obtained and kept on the basis of which the identity and risk factor of the client shall be established;
(d) continuous monitoring of the business relationship with the client, including transactions executed during that relationship (whether the transactions correspond to the type of business and risk of the client and information about that client), as well as keeping the records and documentation on business relationship monitoring;
(e) if possible, and before establishing business cooperation with the client, the reasons for which the client terminates the contractual relationship with another capital market participant shall be determined;
(f) when executing transactions of an identified client using technologies that do not involve direct contact, procedures enabling prior verification of the authenticity and accuracy of the transaction order and the authenticity of its applicant shall be verified.

Establishing and verifying the identity of the representative or authorized person

When establishing a business relationship or executing a transaction by a representative or authorized person (attorney), the identification of the authorized person (representative, attorney) and the client on whose behalf and for whose account the account shall be opened or transaction executed exclusively on the basis of personal identification documents or other public documents, being as follows:

- documents issued in the prescribed form by a state authority within its competence, or an institution and another legal person within the legally entrusted public authority and a written authorization-power of attorney, certified by a notary, consulate, court or state administration authority.

If during the establishment and verification of the identity of the representative, the veracity of the obtained data is doubted, and especially in cases when:

- a written authorization (power of attorney) has been issued to a person who obviously does not have a sufficiently close connection (e.g. family, business, etc.) with the client to execute transactions using the client's account; when the client's financial standing is known, and the funds on the client's account or in connection with that account do not correspond to his financial standing; when during business relations with the client he notices some unusual transactions, his written statement must be obtained.

Identifying a beneficial owner of a legal person

Within the establishment and checking of a client who is a legal person, in addition to identification, the beneficial owner of that legal person shall be also established by implementing measures in order to obtain data for the natural person who is the beneficial owner.

In the case of a high-risk client, confirmation of the obtained data is mandatory, if they were not obtained from a confidential and independent source (e.g. if the only source of data when establishing the client's identity was a written statement of the legal representative, in which case the data are checked to the extent enabling the understanding of the ownership of the legal person entity and the structure of its control, in order to identify all beneficial owners of the client).

Pursuant to the Law on the prevention of money, laundering and terrorist financing the beneficial owner of a company or legal person shall be considered the following:

- a natural person who directly or indirectly owns at least 25% of the shares, voting rights and other rights, on the basis of which he participates in the management, or own more than 25% share of the capital or has a dominating influence in the management of the assets of the business organization or legal person;
- a natural person who indirectly has ensured or ensures funds to a business organization or legal person and on that basis has the right to influence significantly the decision making process of the managing body of the business organization or legal person when decisions concerning financing and business are made.

A beneficial owner of a foreign legal person (trust, fund or similar) that receives, manages or allocates assets for certain purposes, in the context of this Law, shall be considered:

- a natural person who, directly or indirectly controls at least 25% of a legal person's assets or of a similar foreign entity;
- a natural person who is determined or determinable as a beneficiary of at least 25% of the income from the property that is being managed.

Ownership data are obtained on the basis of the original or a certified copy of the excerpt from the electronic database register kept by the Tax Administration issued at the request of the legal representative or authorized person on behalf of the legal person, as well as based on direct verification in the court register or other public register, or through other available sources.

If prescribed information on beneficial owner (e.g. date and place of birth) cannot be obtained from the court register or other official register, the missing data shall be obtained from the legal representative or his authorized person.

When establishing a business relationship, the client is warned about the obligation to provide written notice of any change related to the beneficial owners.

Method of establishing client eligibility

After completing the identification procedure of the client and the beneficial owner, if the client is a legal person, information is obtained on the purpose and nature of the business relationship or transaction and other data in accordance with the Law, the client's acceptability is assessed based on obtained and verified data and client information establishing a business relationship. The assessment of the client's eligibility is usually performed by an employee of the Company who establishes a business relationship. In case there are indicators implying to an increased risk, the employee shall consults with the compliance officer in charge of the prevention of money laundering and terrorist financing or with his deputy.

When all legally prescribed data on the client are identified, or obtained and verified, the Company establishes a business relationship with the client.

In certain cases, the Company may refuse to establish a business relationship with a client, or terminate an already established relationship (in the case of old clients). Such decision shall be made by the Executive Director or a person designated by him, at the proposal of the compliance officer in charge of the prevention of money laundering and terrorist financing or his deputy.

The establishment of the business relationship shall be refused to the following clients:

- If the country of origin of the client or the beneficial owner of the client is listed on the list of non-cooperative countries, or on the list of countries that the supervisory body considers risky based on its own assessment ("off-shore" zone, etc.);
- If the client is a person or the beneficial owner of the client is a person from a country subject to measures under the United Nations Security Council Resolutions;
- If the client is a person from the List, compiled pursuant to the Resolutions of the United Nations Security Council;
- If the client is on the internal list of the Company compiled on the basis of data obtained in communication with the managing bodies;
- If, in addition to undertaking all measures for the purpose of identification, the identity of the actual client is more seriously doubted.

Increased risk of money laundering and terrorist financing is heightened in connection to the clients from certain destinations, and these are especially:

- Countries subject to United Nations sanctions, embargoes or similar measures;
- Countries designated as financing or supporting terrorist activities, as well as those that have certain terrorist organizations operating in them;
- Countries designated by the FATF or other reference international organization as countries lacking an internationally recognized standard for the prevention and detection of money laundering and terrorist financing;
- Countries that, based on the assessment of the competent international organizations, are marked as states with a high level of organized crime due to: corruption, arms trafficking, trafficking in white slaves or human rights violations;
- Countries classified by the international organization (FATF, UN Security Council, etc.) as non-cooperative jurisdictions or territories;
- States representing offshore areas.

c) Other relevant factors

Other factors that may be relevant and affect the risk of money laundering and terrorist financing are as follows:

- legal (related to the national law and potential threats);
- structural (related to certain business models and processes).

Within the above, the following is considered:

- emerging services, i.e. services that have not been previously offered in the financial sector and must be monitored separately to determine the actual level of risk;
- electronic placement of orders for securities trading;
- provision of services to persons with whom a business relationship has not been previously established under the Law;
- provision of services by opening the so-called joint accounts that mobilize funds from different sources and from different clients, and which are deposited in one account opened in one name;
- payment of funds to earmarked accounts, and it is not certain that the service will be performed.

Scoring business-based risk assessment

Once the Company has identifies and documented all the inherent risks, it shall attribute a level to each risk. Pursuant to the size and type of business that the Company is engaged in, it shall establish a

risk scale. Very small businesses (by type and volume of business) performing occasional direct transactions are required to distinguish between low and high risk categories, while larger businesses are expected to establish more risk categories if justified (low, medium, medium-high, high risk, etc.).

By law, every risk identified as high must be addressed with adequate mitigation measures (in-depth client checks and business relationship monitoring) which must be documented.

2. Relationship-based risk assessment

Relationship-based risk assessment is focusing on the client in relation to:

a) products, services and distribution channels the client uses;
b) geographical location of the client's place of residence/seat and his transactions, and
c) client's characteristics and transaction patterns.

Since the risk assessment is based on the inherent characteristics of the Company's client under a) and b) previously processed further analysis focuses on the client's characteristics and transaction patterns

If in the course of business we identify clients whose transactions are sporadic, we will not have much available information on the basis of which we could fully assess the client (as opposed to the client with whom the business relationship lasts and thus provides information, activity patterns, etc.). The risk assessment of such clients is most often focused on monitoring the transaction, as opposed to keeping a client's file in a business relationship that lasts, in order to possibly report a suspicious transaction, in case there is a suspicion of money laundering and terrorist financing.

Some of the criteria that define examples of high-risk clients are as follows:

- the client is interested in paying higher fees to the Company in order to keep certain information about himself secret;
- the client acts through intermediaries such as investment managers, advisors, lawyers or accountants, in order to avoid establishing his own identity;
- the client (natural or legal person) is reluctant to provide information to the Company about the nature and purpose of his business, previous financial connections, expected activities or directors of the legal person or business location;
- the client insists on investing in financial instruments that do not fit his profile and education, even when it is suggested that they are high risk;
- the client refuses to disclose the origin of funds or provides false, misleading or substantially inaccurate information to the Company;
- the client is reluctant to meet the employees of the Company, is very secretive and defends himself when asked to provide additional information;
- the client (natural or legal person) has a residence/seat in a jurisdiction known as a banking secrecy paradise, a tax haven or a high-risk geographical location;
- the client who is not a local resident or comes from a place that is outside the scope of regular clients of the Company;
- the client uses companies from many jurisdictions to open numerous accounts;
- the client (natural/legal person) who is a non-resident uses national accounts for trading on foreign stock exchanges through foreign branches with different controls on prevention of money laundering and terrorist financing and identification practices;
- the client has a history of changing financial advisors or using a number of firms or banks;

- the client does not use the account for the earmarked purposes, or the client's transaction patterns suddenly change in a way that is inconsistent with his regular activities;
- the client (legal person) has no tangible business, income or products, which may suggest that it is a "shell company" used to trade financial instruments;
- the value of financial instruments deposited in the account does not correspond to the client's profile;
- the client expresses unusual concerns regarding the prevention of money laundering and terrorist financing, the Company's policies and reporting obligations to the competent state authorities;
- the company knows or learns that the client is suspected of involvement in illegal activities;
- the client's residence address/seat address is linked to a number of accounts/orders that do not appear to be linked;
- the client's trading patterns suggest that he may have insider information;
- the client receives numerous bank transfers from unrelated third parties, and their profile does not show justified business reasons for accepting deposits from third parties;
- the client makes numerous payments to third parties immediately before or after receiving numerous cash deposits from third parties

Some of the features that define examples of high risk transactions are as follows:

- transfer of financial instruments or funds between seemingly unrelated parties;
- transfer of funds to the accounts of financial institutions or banks other than those originally indicated, especially when those accounts are in other countries;
- transfer of funds (payment/receipt) to/from third parties (national or foreign), especially when the name or the account number of the account holder or payer is not specified;
- transactions in which one party buys financial instruments at a high price and then sells them with significant losses to the other party. This can also be an indicator of market manipulation;
- an account that is dormant for a long time and then suddenly becomes active without an acceptable explanation (surge in the payment of large deposits);
- transactions showing that the client is acting on behalf of a third party or transactions involving an unknown contracting party;
- the client buys a particular investment product without concern for investment objectives or performance or that shows a lack of concern for higher than regular transaction fees.

When a client (national or foreign) is established to be a politically exposed person, it must be determined whether there is a high risk of that person committing money laundering or terrorist financing. If the risk is judged high, that person must be treated as high risk.

Scoring relationship-based risk assessment

Under the relationship-based assessment, every high-risk client (or group of clients) requires the application of special measures.

After the client is checked and reviewed, based on the identified risk factors, the client is classified into a certain category of money laundering or terrorist financing risk.

During the business relationship with the client and the monitoring of his business activities, all data are updated and the client is classified in the appropriate classification category. If it is determined that individual client transactions departs significantly from the normal course of business, an additional analysis of the client's business shall be conducted, in order to determine the reasons for

such departure. Based on the additional analysis, the responsible persons will assess the client's risk profile and possibly reclassify it.

RESULTS OF INHERENT RISKS IDENTIFICATION

Common review and monitoring

In addition to client identification, client review and monitoring measures are also being implemented, particularly with regard to:

- opening a securities account or establishing another form of business cooperation with the client;
- each transaction or for several interconnected transactions in the total amount of EUR 15,000 or more;
- when there is doubt in the accuracy or veracity of the obtained customer identification data;
- any transaction, regardless of the value of that transaction, if money laundering and terrorist financing are suspected in connection with the transaction or client.

The client's review and monitoring measures are:

- identification of the client and the beneficial owner, if the client is a legal person;
- obtaining and verifying data on the client, or the beneficial owner, if the client is a legal person;
- obtaining information on the purpose and nature of the business relationship or transaction; and
- after the establishment of a business relationship, regular monitoring of the client's business activities and checking the compliance of these activities with the nature of the business relationship and the usual scope and type of the client's business.

Enhanced verification and monitoring

This type of verification of the client shall be carried out in the following cases:

- if the client is politically exposed person;
- if the identification of the client is carried out in his absence.

Client is Politically Exposed Person (PEP)

The status of PEPs and members of their immediate family and close associates is determined in one of the following manners:

- filling in a written form by the client;
- collecting information from public sources;
- collecting information based on insights into databases that include lists of PEPs (e.g. List of PEPs on the website of the Administration, World Check PEP List, etc.);
- collecting information based on the insight into the records of the Agency for the Prevention of Corruption.

Determining close associates of politically exposed persons is applied if the relationship with the associate is publicly known.

Prior to establishing a business relationship with the PEP, the following actions shall be carried out:

- collecting data on the source of funds and assets subject of the business relationship, or transactions, based on personal and other documents submitted by the client, and if the prescribed data cannot be obtained from the submitted documents, data shall be obtained directly from the client's written statement;

- obtained written consent of the Executive Director, prior to establishing a business relationship with the client.

Establishing client's identity in his absence

When determining and verifying the identity of a client who is not present, the following additional measures shall be undertaken:

- additional documents, data or information shall be obtained, on the basis of which the identity of the client is verified;
- submitted documents shall be checked or a certificate shall be obtained from the financial organization that performs the payment transaction that the first payment of the client was made debiting the account kept with this organization.

STEP 2: CREATION OF KEY CONTROL MECHANISMS AND RISK-REDUCTION MEASURED

Risk mitigation is narrowed down to implementing control measures aimed at limiting the risks of money laundering and terrorist financing that we have identified while conducting the risk analysis.

Overall expectations are that the risk mitigation measures and control mechanisms will stay within the risk limits that we have identified.

Pursuant to identified situation, the Company should conduct internal controls that will help mitigate the overall risk.

In business-based risk analysis, elements that we have identified as high-risk should be documented and mitigated by controls and appropriate measures.

It is important to continuously monitor the accounts and transactions of clients in order to prevent money laundering and terrorist financing, and to keep records of data and measures that we are implementing. In the light of the above, information on the client's business is collected and the conformity of transactions with the client's profile is assessed. Special attention is paid to all complex, unusually high transactions and all unusual types of activities that do not have an obvious economic or legal purpose. In determining the above, we are using the List of Indicators of Suspicious Transactions, representing an integral part of this document.

RESULT OF CREATION OF KEY CONTROL MECHANISMS AND RISK-REDUCTION MEASURES

As a result of the above:

- data on the client's identity and actual ownership are regularly updated;
- an adequate level of monitoring business relations has been established and is being implemented (less frequent monitoring for lower risk clients and more frequent for high-risk clients);
- adequate mitigation measures are being implemented in cases where the risk of money laundering and terrorist financing is high.

STEP 3: RESIDUAL RISKS EVALUATION

Residual risk is the risk remaining after we have implemented the risk mitigation measures and control mechanisms. Regardless of how strong our risk management program and risk mitigation measures are, our business will always have some exposure to residual risks which we are obliged to manage.

Mitigated risks are still risks, they have been reduced, but they have not been completely eliminated. Hypothetically, the electronic transaction tracking and control system may fail, causing a failure to record certain transactions that may be related to money laundering and terrorist financing.

Residual risk management should include:

- carrying out of additional internal confirmations of certain transactions, and
- monitoring certain transactions more frequently to reduce the structuring risk (e.g., transaction worth EUR 15,000.00 is divided into two transactions in the amount of EUR 7,500.00 each to avoid the obligation to report a transaction).

RESIDUAL RISKS EVALUATION RESULTS

Proper assessment of the level of residual risks is providing us the opportunity to adequately manage them.

STEP 4: RISK-BASED APPROACH IMPLEMENTATION

We need to apply a risk-based approach on a regular basis as a part of our day-to-day activities. In order to be effective, the Company's risk analysis must be documented in accordance with legal obligations.

A risk-based approach allows the Company to focus on those customers who pose the greatest potential risk. In order to implement it, it is necessary that all employees who have direct contact with clients understand the Company's compliance policies and procedures. In the light of the above, the Company's compliance policies and procedures contain requirements regarding:

- reporting;
- record keeping;
- client identification;
- risk assessment; and
- special measures (enhanced verification and monitoring of client's business) for high risk cases.

Policies and procedures also:

- explain the manner of detecting suspicious transactions and the method of taking actions for dealing with such situations;
- determine and explain what kind of monitoring is done for particular situations (low risk against high-risk clients/business relationships);
- describe all aspects of your monitoring:
    - when it is done (frequency),
    - how it is conducted, and
    - how it is checked.

The risk management and risk mitigation approach requires the leadership and commitment of the Company's senior management. A risk management system is being established and gradually developed.

RISK-BASED APPROACH IMPLEMENTATION RESULTS

The risk-based approach implies that the Company:

- Based on the risk analysis is describing the process of the risk-based approach, frequency of monitoring business relationships for low-risk and high-risk clients, as well as the measures and controls it applies to mitigate the high risks identified under Step 1;
- Applies a risk-based approach in the manner prescribed by the Company's acts;
- Updates documentation containing information on the identity of clients and actual ownership;
- Monitors all business relationships;
- Conducts more frequent monitoring of business relationships for clients at high risk of money laundering and terrorist financing;

- Implements special measures prescribed by law for high-risk clients.

STEP 5: REVIEW OF THE RISK-BASED APPROACH

An integral part of the Company's risk analysis is the periodic review of the risk-based approach (minimum every 2 years) aimed at testing the efficiency of the compliance regime, which includes the verification of:

- company's policies and procedures;
- company's risk assessment related to money laundering and terrorist financing; and
- training (professional development) for employees and senior management.

Should the Company's business model change, it is also required to update the risk analysis according to new products or services, together with risk mitigation policies, procedures and measures.

Verification of the risk-based approach covers all components of the Company's operations. The risk-based approach has dynamic properties, it changes, evolves over time depending on the emergence of new products or new threats in the Company's operations. Proper and timely compliance and implementation of this step is essential for the implementation of an efficient risk-based approach.

RESULTS OF THE RISK-BASED APPROACH REVIEW

The Company carries out:

- Checking the risk-based approach at least once every two years as well as when there are changes in the business model (offering new products or services)
- Verification of a risk-based approach covering all compliance policies and procedures, analysis of money laundering and terrorist financing risks and vocational training (training) to test their effectiveness.
- Checking access by documenting all information
- Results of verification of the risk-based approach also by documentation, together with corrective measures and follow-up activities.

INFORMATION SYSTEM IN THE CLIENT RISK ASSESSMENT SUPPORT SERVICE

The widespread use of new technologies, which enable anonymity (internet banking, use of ATMs, etc.), for the purposes of rapid cash flow, has contributed to further complicating investigations into suspected money laundering or terrorist financing.

The establishment of an appropriate information system that provides automated support for client risk assessment, continuous monitoring of client business relations and transaction control, as well as timely submission of information, data and documentation to the Company's management, is providing for a significant contribution to risk-based approach in combating money laundering and terrorist financing.

The company must, when performing money transfer services, collect the following information about the payer as mandatory:

- Name of the payer's legal person of the payer, i.e. first and last name of the natural person of the payer;
- Seat of the payer's legal person, i.e. permanent or temporary residence address of the payer's natural person (these data may be replaced by the date and place of birth of the payer's natural person, payer's identification number and unique registration number of the legal person, or unified citizens identification number or JMBG of a natural person who performs business activity, or JMBG of a natural person who does not perform business activity);

- Account number (if the payer does not have an account, the Bank shall replace the account number with an identifier that allows monitoring the implementation of transfers from the payer.

The Company shall determine whether all data on the payer are entered in the form or message that accompanies the electronic transfer of funds. When the Company assesses that the lack of accurate or complete information about the payer is the basis of suspicion in money laundering or terrorist financing, it shall immediately inform the competent authority of the Company.

The Company shall establish and verify the identity of the payer in each case, regardless of the amount and type of transaction when there are grounds for suspicion in money laundering and terrorist financing, and shall immediately notify the compliance officer.

APPOINTMENT OF COMPLIANCE OFFICERS

The Law on Prevention of Money Laundering and Terrorist Financing stipulates the obligation of appointing the compliance officers who are responsible in the Company for the implementation of measures and tasks set forth in the Law. Pursuant to this obligation, the Company shall appoint a compliance officer for the prevention of money laundering and terrorist financing and his deputy. Exceptionally, a company with three or fewer employees shall not be obliged to appoint a deputy compliance officer.

The Company provides appropriate conditions for compliance officers to perform their tasks, being as follows:

- establishment, functioning and development of a system for detecting and preventing money laundering and terrorist financing;
- proper and timely submission of data to the Administrative authority and cooperation in the inspection supervision procedure;
- initiates and participates in the development and amendments to operational procedures and internal acts of the Company related to the prevention and detection of money laundering and terrorist financing;
- cooperation in the development of guidelines for conducting checks related to the prevention and detection of money laundering and terrorist financing;
- monitoring and coordinating the activities of the Company in the field of detection and prevention of money laundering and terrorist financing;
- cooperation in the establishment and development of information technology for the detection and prevention of money laundering and terrorist financing;
- submission to the Board of Directors and the Executive Director initiatives and proposals for improving the system of detection and prevention of money laundering and terrorist financing;
- development of professional training and development programs for employees, related to the detection and prevention of money laundering and terrorist financing;
- development and submission of reports to the Board of Directors once a year, and more frequently if necessary.

PROFESSIONAL TRAINING AND DEVELOPMENT OF EMPLOYEES

Pursuant to the legal obligation, the Company shall take care of professional training and development of employees in order to prevent money laundering and terrorist financing. Professional training and development of employees includes, primarily the in-depth knowledge of the provisions of the Law and subordinate legislations adopted on the basis of the Law, internal acts of the Company, international standards arising from international conventions in the field of prevention of money laundering and terrorist financing, guidelines and indicators for identifying suspicious transactions, as well as obligations to notify competent authorities and

records keeping. Professional training and development of employees related to the prevention of money laundering and terrorist financing, aims at raising the awareness of employees about the importance of timely measures to prevent money laundering and terrorist financing.

The Company has established a system of professional training and development of employees for keeping them informed about new things, including current techniques, methods and trends in the field of prevention of money laundering and terrorist financing, and provides clear explanations of all aspects of the Law and obligations regarding prevention of money laundering and terrorist financing, and in particular requirements pertaining to an in-depth analysis of the client, and notification of suspicious transactions.

Training of employees, related to the prevention of money laundering and terrorist financing, includes a good knowledge of regulatory requirements (Laws and subordinate legislations) and internal policies and procedures adopted by the Company for successful risk management in this area.

RECORDS KEEPING, PROVISION OF PROTECTION AND KEEPING DATA AND DOCUMENTATION

The Company keeps records, provides protection and keeps data and documentation on all persons and transactions, which includes data and documentation related to account opening, establishment of business cooperation, as well as executed transactions. These data and documentation are kept in written and electronic form for ten years from the date of execution of the transaction or termination of business cooperation.

Data on transactions for which there are grounds for suspicion of money laundering or terrorist financing shall be immediately submitted by the compliance officer to the Administration authority.

Employees of the Company must not disclose that the information or documentation about the client or the transaction it performs has been or shall be disclosed to the Administration authority or that the Administration has temporarily suspended the transaction or issued an order for continuous monitoring of accounts. Data on the request, submission of data, information or documentation and temporary suspension of the transaction and continuous monitoring of the account shall represent an official secret.

Requests of the Administration for submission of data, as well as responses to them, shall be recorded and kept according to a special procedure and the request shall be designated as a secret by the Administration, while data on suspicious transactions shall be designated as a “top secret”. A special logbook for opening these documents shall be opened, and they shall be kept in a specially protected locker, separate from other documents. The data submitted to the Administration in electronic form shall be copied, and electronic records shall be also kept under the same regime.

Data and documentation obtained under the Law shall be kept for 10 years after the execution of the transaction, closing of the account or termination of the contract.

Data and documentation on the compliance officer and his deputy, professional training and development of employees and implementation of internal control under the Law shall be kept for four years after the appointment of the compliance officer and his deputy, performed professional training and development of employees and internal control.

Previously obtained data shall be kept in the manner as documentation on clients and transactions submitted to the Administration.

REPORTING

The compliance officer must submit a report on the activities on the prevention of money laundering and terrorist financing once a year, and more frequently if necessary.

The report should contain in particular information on:

- total number of submitted reports on suspicious transactions;
- total number of suspicious transactions analyzed by employees of the Company, and about which, based on the review and assessment of the compliance officer, the Administration was not notified;
- total number of suspended transactions;
- total number of issued orders for continuous monitoring of client accounts;
- newly discovered ways and techniques of money laundering with a proposal of measures for their identification and detection;
- activities undertaken in resolving problems observed in the application of procedures and practices for identifying suspicious transactions;
- results of the training of employees with information on the date of the training, topics covered and list of participants who attended the training;
- proposing measures to improve policies and procedures for detecting and preventing suspicious transactions.

The report, after adoption by the Board of Directors, shall be submitted to the Administration authority.

ENTRY INTO FORCE

This Act shall enter into force on the date of its adoption.

No: _____
Podgorica, 10 January 2020

PRESIDENT OF THE BOARD OF DIRECTORS

Ivan Jokanović

Appendix 1: Checklist

The checklist is appropriate for smaller reporting entities and it represents a baseline used by the Company given the nature and scope of business. It is an example of an initial risk assessment of a customer, product, service, business and geographic area.

CLIENTS RISK

Is the Company having clients who are…		
engaged in cash-intensive business?	YES	NO
residing outside Montenegro?	YES	NO
who are intermediaries or persons carrying out professional activities and holding for clients where the identity of the beneficial owners has not been established?	YES	NO
unregistered charities or other unregulated “non-profit” organizations (especially those operating on a “cross-border” basis)	YES	NO
residing in an area known to have a high crime rate?	YES	NO
offering on-line gambling?	YES	NO
whose nature of business makes it more difficult to identify beneficial owners?	YES	NO
foreign politically exposed persons?	YES	NO
do not have an address or have several addresses without justified reason?	YES	NO
known to be involved in criminal activities?	YES	NO
having connections with organized crime?	YES	NO

PRODUCTS/SERVICES RISK

Is the Company offering products and services which are...		
making more difficult full identification of clients?	YES	NO
of help in the establishment of trade companies?	YES	NO
lending the address to foreign legal persons?	YES	NO
doing business for the purpose of concealing the client's beneficial owner?	YES	NO
Executing real estate transfers between the parties in an unusually short time without obvious legal, commercial or other justified reason?	YES	NO
providing services related to the establishment, operation or management of inactive fictitious companies and companies in regular ownership?	YES	NO

BUSINESS RELATIONSHIP RISK

Is the Company executing...		
transactions for which you establish and verify identity without the client's presence and/or establish a business relationship without the client's presence?	YES	NO
Is the Company engaged in activities pertaining to...		
complex financial transitions?	YES	NO
payments to/from third parties and cross-border payments?	YES	NO
high-risk real estate transactions?	YES	NO
cash transactions?	YES	NO

GEOGRAPHICAL RISK

Is the Company operating or conducting activities in the following countries...		
in a country that is not a member of the EU or a signatory to the Agreement on the European Economic Area?	YES	NO
in a country against which the UN has imposed sanctions, embargoes or similar measures?	YES	NO
in a country known as a tax haven or a financial offshore center?	YES	NO
in a country identified by the FATF as non-cooperative in the fight against money laundering or terrorist financing?	YES	NO
in a country where terrorist activities take place?	YES	NO
in a country supporting terrorist activities?	YES	NO
in a country where, in the opinion of relevant international organizations, appropriate AML/TF measures are not implemented?	YES	NO
in a country known for significant level of corruption or other criminal activity?	YES	NO