Pursuant to Article 48 paragraph 1 Law on Prevention Money Laundering and Terrorist Finansing ("Official Gazette of Montenegro" no. 033/14, 044/18 and 073/19), the Board of Directors on XXIV regular session held on March 21, 2022 adopted:

PROGRAM OF MEASURES FOR IMPLEMENTING MEASURES TO PREVENT MONEY LAUNDERING AND TERRORIST FINANCING

Ver 04-2022

March 2022

Finveo
The Capital Plaza, Cetinjska 11
81000 Podgorica, Montenegro
T +382 20 436 698
info@finveo.mn • www.finveo.com

Contents

Finveo
The Capital Plaza, Cetinjska 11
81000 Podgorica, Montenegro
T +382 20 436 698
info@finveo.mn • www.finveo.com

Finveo
The Capital Plaza, Cetinjska 11
81000 Podgorica, Montenegro
T +382 20 436 698
info@finveo.mn • www.finveo.com

1. Terms and definitions

Certain terms used in this document have the following meanings:

- The client is a domestic or foreign legal entity, company, natural person, entrepreneur, foreign trust and another person, or an entity equated with him who performs a transaction or establishes a business relationship with the obligor;
-AML officer, ie his Deputy is a person appointed by the obligor with authorizations and responsibilities for the implementation of measures and actions taken for the prevention and detection of money laundering and terrorist financing;
- **A transaction** is the receipt, investment, exchange, safekeeping or other disposal of money or other property;
- A**n occasional transaction** is a transaction executed by a client who is not in a business relationship with the Company;
- **A cash transaction** is any transaction in which the taxpayer receives cash from the client, ie hands over the cash to the client in possession and disposal;
- S**uspicious transaction** is any transaction with assets for which it is assessed on the basis of indicators for recognizing suspicious transactions or on the basis of other circumstances and facts, that they represent proceeds of crime or in connection with a transaction, assets, property or the person performing it. for suspected money laundering or terrorist financing;
- **Money laundering and terrorist financing risk** is the risk that a client will use a financial system for money laundering or terrorist financing, ie that a business relationship, transaction or product, service will be used, directly or indirectly, for money laundering or terrorist financing;
The correspondent relationship is:
- the relationship between one bank as a correspondent providing banking services to another bank as a respondent including the provision of current or other account liabilities or related services, such as cash management, international cash transfers, check settlement, transitory accounts, and foreign exchange services; and
- the relationship between and within credit institutions and financial institutions, including similar services provided through correspondent and respondent institutions, including relationships established for securities transactions or cash transfers;
- **A quasi-bank** is a credit institution, ie another similar institution that is registered in a country where it is not present, does not perform business, has no business premises, employees, management bodies, management and which is not related to a financial group subject to supervision to detect and prevent money laundering. money or terrorist financing;
- **A politically exposed person** is a person as defined in Article 32 of the Law on Prevention of Money Laundering and Terrorist Financing;
- Property means property rights of any kind, whether they relate to goods of a tangible or intangible nature, movable or immovable property, securities and other documents (in any form, including electronic or digital form) proving property rights ;
- Assets are financial assets and benefits of any kind including:
- cash, checks, cash receivables, bills of exchange, remittances and other means of payment;
- funds invested with taxpayers;
- financial instruments determined by the law regulating the capital market which are traded with an appropriate offer, including shares and stakes, certificates, debt instruments, bonds, guarantees and derivative financial instruments; - other documents proving the rights to financial resources or other financial sources; - interest, dividends and other income from funds;
- receivables, loans and letters of credit;

- A business relationship is a business, professional or commercial relationship that is related to the professional activities of the Company which at the time of establishment are expected to be of a permanent nature
- An anonymous company is a foreign legal entity with unknown owners and / or managers; the person is a domestic or foreign natural or legal person
- A predicate criminal offence is a criminal offence by the commission of which a profit was made which may be the subject of a criminal offence of money laundering;
- **Trust or company service provider** is a person who performs the activity of providing services to third parties, and in particular:

- establishment of companies or other legal entities;
- performing the functions or appointing another person to perform the function of a trust trustee established by an explicit statement or a similar legal entity of foreign law;
- provision of headquarters services, business addresses and other related services;
- performing the function or enabling another person to perform the function of a trustee of a fund or similar legal entity of foreign law that receives, manages or distributes assets for a specific purpose, except for the investment pension fund management company;
- performing the function or appointing another person to perform the function of a nominal shareholder on behalf of another person, except for a company whose shares are listed on a regulated market which is subject to publication in accordance with European Union regulations or equivalent international standards;

- Distribution channel is a channel used to deliver products and services to the last user;
- Cash are banknotes and coins that are in circulation as legal tender;

- Information on the client's activity is any data on the client, regardless of whether it is a private or professional status or activity of the client;
- **The Police Directorate - Sector for the Prevention of Money Laundering and Terrorist Financing** (hereinafter the AML Agency - is a central financial intelligence unit that receives, collects, stores, analyses and submits data, notifications, information and documentation, as well as the results of operational analyses of suspicious transactions to the competent authorities for further action in order to prevent money laundering and terrorist financing, in accordance with the Law.

2. Introduction

2.1. Strategic principles

Montenegro is part of the Balkan route - the main trade corridor through which, among other things, criminal activities take place, such as: drug trafficking, human trafficking, etc. In the countries of the wider region, the income from these activities is sometimes "laundered" through certain schemes of private companies, in some cases even public companies. International regulations, European Union law and laws of Montenegro (Law on Prevention of Money Laundering and Terrorist Financing, with bylaws) oblige the Company to build and maintain a system that will contribute to the overall monitoring of financial transactions and provide assistance to part of the proceeds from criminal activities. income that finances terrorist activities, does not end up in legal cash flows in Montenegro or abroad.

Although cash is rarely deposited in securities accounts, the securities industry is unique in that it can be used to launder funds acquired elsewhere and to generate illegal funds in the industry itself through fraudulent activities. Examples of types of fraudulent activities include insider trading, market manipulation, Ponzi schemes, cybercrime, and other investment fraud.
Respecting the foregoing, the Company complies with all international and national embargo regulations and other restrictive measures, as well as national regulations derived from them. Also, there is a ban on financing any form of illegal trade in weapons and military equipment, terrorism, drug trafficking, child labour, human trafficking, gambling, dual-use trade, etc., as well as a ban on doing business with all individuals and legal entities that are involved in these illegal activities.
In order to effectively implement measures to prevent money laundering and terrorist financing, the Company must know its customers and their activities. Accordingly, the application of the "Know Your Client" principle is a priority in preventing money laundering and terrorist financing. The application of adequate measures of knowledge and monitoring of clients' operations provides an opportunity for quality analysis of potential risks of money laundering and terrorist financing, respecting the rule that the scope of applied measures of knowledge and monitoring of client's business relations and transaction control depends on specific money laundering and terrorist financing risks. business relationship, product, or transaction. High risk requires the mandatory application of enhanced measures of knowledge and monitoring of the client's business relationship and control of transactions, while low risk allows the application of simplified measures of knowledge and monitoring of the client's business relationship and control of transactions.

The above principles form the basis of the system established by the Company for risk management of money laundering and terrorist financing.

2.2. Purpose and goals of the program

The goal of the Program of Measures to Prevent Money Laundering and Terrorist Financing (hereinafter: the Program) is to provide a unified understanding of the tasks, legal requirements, measures and actions necessary to prevent money laundering and terrorist financing, and in particular:

- to prevent money acquired in unlawful and illegal transactions through financial transactions from hiding its true origin and from being introduced into legal cash flows;
- to establish a strong internal organization and cooperation between organizational units and employees in the process of data collection, processing and storage;
- to define activities aimed at preventing money laundering and terrorist financing so that they can be included in appropriate work processes;
- to establish an efficient and effective system for managing the risk of money laundering and terrorist financing according to the size and type of clients with which the Company does business, as well as the types of products and services it offers.

2.3. General aspects

In regards to the Law on the Prevention of Money Laundering and Terrorist Financing, money laundering is considered to be:

1) exchange or transfer of money or other property with knowledge that they originate from criminal activities, or from acts of participation in those activities, with the aim of concealing or falsely presenting the illegal origin of property, or providing help to a person involved in criminal activities, in order to avoid sanctioning his behaviours;

2) concealment or misrepresentation of the nature, origin, location, movement, disposal or ownership of money or other property, with the knowledge that they originate from a criminal activity or participation in that activity;

3) acquisition, possession or use of property with the knowledge that at the time of receipt of the property originates from a criminal offence or participation in that offence;

4) participation in the execution, association for the purpose of execution, attempted execution and assistance, encouragement, facilitation and counselling in connection with the execution of the activities referred to in item 1, 2 and 3 of this article.

These activities performed in other countries are also considered to be money laundering activities.

Terrorist financing is considered to be:

1) securing or collecting, or attempting to secure or collect money or other property, directly or indirectly with the aim or knowledge that they will be used in whole or in part for the implementation of a terrorist act =, or used by a terrorist or terrorist organization;
2) inciting or assisting in the provision or collection of funds or property, with the aim that they will be used to carry out a terrorist act or used by a terrorist or terrorist organization.

Dirty money is considered to be any money acquired by a criminal offence, as well as all property coming from that money (tangible and intangible). Money laundering is always preceded by some of the criminal activities, that is, money laundering without criminal activity does not exist.
The money laundering procedure implies that funds originating from criminal activities are inserted into the legal system,

1. by placing them in a way that enables them to quickly and easily conceal the origin of funds,
2. their stratification and
3. finally, the final integration.

Placement implies the introduction of illegally acquired money or other valuables into the financial or non-financial system of a country, using financial and non-financial legal entities, ie institutions.
Stratification is the concealment of illegally placed sources of funds through various products and services of financial institutions through financial transactions. This phase of money laundering is the concealment of sources of funds, through fictitious business activities (trade and services). Stratification is the most complex part of the money laundering process and is most often carried out through various typologies (conversion - currency trading, securities trading through custody accounts, non-existent services, redemption of receivables, etc.), of course with the possibility of greater anonymity.

Integration is the final phase in which laundered assets are integrated and placed in legal economic flows, as a result of seemingly legitimate business activities (for example, real estate investments, valuables, companies, etc.).
In order to launder money, all these phases mostly overlap, which means that it is difficult to define clear phases of placement, stratification and integration.

3. Organizational framework

3.1. Legal framework

In a positive legal sense, the Program is based and implemented together with:

- Law on Prevention of Money Laundering and Terrorist Financing ("Official Gazette of Montenegro", No. 033/14, No. 044/18, No. 73/2019 and No. 070/21 (hereinafter: The Law)
- Guidelines for a risk-based approach and risk analysis of money laundering and terrorist financing for capital market participants, published on the website of the Capital Market Commission http://www.scmn.me/images/files/SPNFT/Guidelines-- -October-2019.pdf;
- Guidelines for risk analysis with banks to prevent money laundering and terrorist financing ("Official Gazette of Montenegro", No. 022/19),
- Rulebook on the manner of work of the AML officer, manner of conducting internal control, storage and protection of data, manner of keeping records and training of employees ("Official Gazette of Montenegro", No. 071/20)
- Rulebook on conditions and manner of submitting data on cash, suspicious and other transactions to Financial Intelligence Service ("Official Gazette of Montenegro", No. 053/21)
- Rulebook on the list of indicators for identifying suspicious clients and transactions ("Official Gazette of Montenegro", No. 141/21)
- Law on International Restrictive Measures ("Official Gazette of Montenegro", No. 056/18)
- Law on electronic identification and electronic signature ("Official Gazette of Montenegro", No. 031/17, 072/19)
- Policy and procedure for money laundering and terrorist financing risk
- Know Your Client (KYC) procedure

3.2. Scope

The application of this Program is mandatory for all employees of the Company. Violation of the rules established by this Program is subject to disciplinary liability of employees.

3.3. Organizational bases

The Company is obliged to appoint an Authorized Person for the Prevention of Money Laundering and Terrorist Financing (hereinafter: the AML officer) and at least one deputy for the activities of detecting and preventing money laundering and terrorist financing. The AML officer independently performs tasks and is directly responsible to the Board of Directors of the

Company, and functionally and organizationally separated from other organizational parts of the Company. The Deputy of AML officer replaces the AML officer in his absence and performs other tasks in accordance with the general and other internal acts of the Company.
For the efficient execution of tasks related to the establishment, operation and development of the system for detecting and preventing money laundering and terrorist financing, the Company is obliged to provide the AML officer and his deputy with:

- unlimited access to data, information and documentation necessary to perform their tasks;
- appropriate material and other working conditions;
- appropriate spatial and technical working conditions that ensure an adequate level of protection of confidential data and information at their disposal;
- appropriate information and technical support that enables continuous and reliable monitoring of activities in the field of prevention of money laundering and terrorist financing;
- continuous professional development;
- protection from actions that may affect the smooth performance of their duties;
- assisting and supporting the conduct of business and reporting on facts relevant to the detection and prevention of money laundering and terrorist financing.

The Company is obliged to submit to the Administration for the Prevention of Money Laundering and Terrorist Financing (hereinafter: the AML Agency) within 8 days from the date of appointment of the AML officer and his deputy an act of appointment containing personal data and job title of the AML officer and the person designated for his deputy and to notify the AML Agency of any change in this information, without delay, and no later than within 15 days from the day of their change.

3.3.1. Tasks and duties of the AML officer

1. Ongoing activities to prevent money laundering and terrorist financing:

   - establishment, operation and development of a system for detecting and preventing money laundering and terrorist financing, as well as proposing initiatives for its improvement,
   - deciding on the establishment and duration of business relationships;
   - monitoring existing customer relationships,
   - continuous monitoring of customer transactions,
   -proper and timely submission of data, information and documentation and acting at the request of the AML Agency,
   - cooperation in the external supervision procedure,
   -assessing the impact of changes in business processes such as the introduction of new products, new practices, including new distribution channels, the introduction of new technology for new and existing products, services or organizational changes, on money laundering and terrorist financing risk exposure,
   - checks of data on persons and entities by querying the database from the list of sanctions that are integrated into the AML / FT tool Sanction Scanner,
   - updating the internal PEP list,
   - updating the internal blacklist,

- updating the Country Survey according to country- or geographical-related risk factors area,
- daily monitoring of the official website of the AML Agency: https://aspn.gov.me,
- answering employee inquiries.

2. Consultations on strategic issues:

- consultations with the Board of Directors regarding business decisions related to the prevention of money laundering and terrorist financing,
- constant monitoring of market trends and typologies of money laundering and terrorist financing,
- assistance with strategic corporate decisions (e.g. products, processes) to the extent that they relate to the prevention of money laundering and terrorist financing,
- cooperation with the competent state bodies in the procedure of application of legal provisions in case of need for additional interpretation.

3. Analysis of complex and unusual / suspicious cases (transactions / clients):

- analysis of complex and unusual / suspicious cases identified by employees,
- analysis of independently identified complex and unusual / suspicious cases (which are the result of constant monitoring of the client's business and control of transactions),
- making an official note of complex and unusual / suspicious cases,
- reporting suspicious transactions or persons to the AML Agency,
- giving a proposal / order for termination of business relationship.

4. Organizing and conducting trainings;

- Development of the Program of professional training and advanced training of employees in the field of detection and prevention of money laundering and terrorist financing,
- Providing adequate training materials,
- Conducting trainings (initial trainings and trainings under the Vocational Training Program and training of employees in the field of detection and prevention of money laundering and terrorist financing).

5. Development and updating of internal acts;

- monitoring requirements and amending the regulatory framework;
- monitoring international standards and practices related to the prevention of money laundering and terrorist financing,
- preparation of internal acts, their harmonization and updating in accordance with the regulatory framework, as well as the size and type of clients with which the Company does business, products and services it offers.

6. IT System

- initiating the application of the necessary IT systems in the function of efficient risk management,

- application, adaptation, quality assurance and improvement of IT systems.

7. Reporting
   - reporting to regulatory authorities (, Capital Market Authority and AML Agency),
   - preparation of internal reports (regular / if necessary).

3.3.2. Tasks and duties of the employees

A money laundering and terrorist financing risk management system can be effective and efficient if all employees actively participate in that system and if they know their clients sufficiently to assess the risk and analyse their business. In that context employees have an obligation to perform the following tasks:

- implementation of work activities prescribed by internal acts;
- monitoring, control, supervision and validation of existing business relationships, ie. transaction, in accordance with the determined degree of risk, including obtaining the necessary data and documentation;
- application of the "Know your client" principle;
- identifying and reporting to the AML officer on suspicious and complex and unusual transactions;
- obtaining information and documentation at the request of the AMl officer;
- regular attendance at trainings.

The employee in charge of establishing and managing the business relationship with the client is primarily responsible for the adequate application of actions and measures of knowledge and monitoring of the client's business and control of transactions.
Employees, including employees with access to data records and documentation obtained in the implementation of measures and tasks related to money laundering and terrorist financing risk management, must not disclose to a client or a third party that:

- the transaction or client has been reported or will be reported to the AML Agency on suspicion of money laundering and terrorist financing;
- the AML Agency temporarily suspended the transaction, i.e. gave instructions to the Bank in this regard;
- the AML Agency required regular monitoring of the client's operations;
- A client or third party has been or could be investigated for money laundering or terrorist financing.

In cases where the Company rejects the request to establish a business relationship, the employee may not explain to the client the reasons for inadmissibility and refusal to enter into a business relationship. In that sense, the notification must be oral and must not hurt or discriminate against the potential client. If the request for establishing a business relationship is rejected, an appropriate level of discretion is required so as not to harm the potential client and the Company's image.

4. Risk analysis

Risk analysis of clients or groups of clients and business relationships is a key preventive element in the system of detecting the prevention of money laundering and terrorist financing. The main

task of the approach based on money laundering and terrorist financing risk is for the Company to identify and assess the exposure to money laundering and terrorist financing risk, as well as to establish appropriate internal control measures and systems, which will enable adequate management and mitigation of this risk.
The risk assessment process involves assessing each individual risk factor and performing an overall risk assessment of the client. Depending on the risk factors, based on which the degree of risk of an individual client or group of clients is determined (client risk factors, risk factors related to business relationships, transactions, services, distribution channels or products, as well as country-specific risk factors or geographical area), all clients can be classified into the following groups:

- Clients with lower risk A,
- Clients with medium risk B,
- Clients with higher risk C.

The degree of identified risk posed by a particular business relationship or transaction determines the scope of applies measures to know and monitor the client's business and control transactions.
The risk assessment procedure is defined in more detail by the Risk Analysis for the Prevention of Money Laundering and Terrorist Financing (hereinafter: the Analysis).

5. Measures to establish and verify the client's identity, monitor the business relationship and control the client's transactions

5.1. Standard measures for establishing and verifying the client's identity, monitoring the business relationship and controlling the client's transactions

Measures to determine and verify the identity of the client, monitoring the business relationship and control of transactions imply the obligation of the Company to:

1) determine and verify the identity of the client on the basis of documents, data and information from credible, independent and objective sources and collect data on the client, ie verify the collected data on the client on the basis of credible, independent and objective sources ("client identification")
2) determine the beneficial owner of the client and verify his identity, including the measures necessary to determine the ownership and control structure of the client;
3) obtain data on the purpose and nature of the business relationship or the purpose of the transaction, as well as other data more precisely defined by this act;
4) regularly monitors the business relationship, including the control of the client's transactions during the duration of the business relationship with the Company and checks their compliance with the nature of the business relationship and the usual scope and type of business of the client.

Measures to determine and verify the identity of the client, monitor the business relationship and control transactions, the Company implements in the following cases:

1) when establishing a business relationship with a client;
2) in the case of one or more related occasional transactions in the amount of EUR 15,000 or more;
3) during each occasional transaction representing the transfer of funds in the amount of EUR 1,000 or more;
4) when there is a doubt in the accuracy or credibility of the obtained data on the identity of the client and the actual identity of the client;
5) when there is a basis for suspicion of money laundering and terrorist financing in relation to the transaction or client.

Measures related to the identification of the client stated above, including verification of the identity of the client's representative and authorized person, identification of the beneficial owner, obtaining information on the purpose and nature of the business relationship or the purpose of the transaction and other prescribed data, are carried out before conducting business relationship and before execution transactions. If the Company cannot perform the prescribed measures, the business relationship may not be established, and if the business relationship is established, the Company is obliged to terminate the business relationship and the transaction may not be performed. In these cases, the Authorized Person, based on the information and data on the client and / or transaction collected so far, may prepare a report on the suspicious client or transaction and submit it to the AML Agency.

If during the implementation of measures to establish and verify the identity of a client who can be a private individual or legal entity the employee doubts of the truthfulness of the obtained data or authenticity of documents, the employee needs to obtains a written statement confirming the truthfulness of the collected data and notice of the AML officer and Deputy without delay, who give binding recommendations regarding the establishment of a business relationship with the client.

5.2. Determining and verifying the identity of a natural person

Determining and verifying the identity of a client who is a natural person, , is done by inspecting a valid personal biometric document of the client (ID card /Driving license/ Passport), in his presence. The employee of the Company who conducts the identification procedure is obliged to obtain a copy of the client's personal biometric document on which he enters the date, time, his name and signature.,
For minors under the age of 18, it is not possible to open an account.
It is not allowed to establish a business relationship with a natural person client on the basis of authorization.
The Company will not establish a business relationship with entrepreneurs or individuals who perform activities.
In the process of identifying a client who is a natural person, , the following information must be obtained:

Data on the client to a natural person	
	• Name;

Data on the client to a natural person	• address of residence or stay; • date and place of birth; • tax number of the natural person; • number, type and name of the body that issued the identity document; • purpose and presumed nature of the business relationship, including information on the client's activity or client status (occupation - employed, unemployed, student, pensioner, farmer, etc.); • Date of establishing business relationship
Transaction data	• date and time of transaction execution; • the amount of the transaction and the currency in which the transaction was made; • purpose of the transaction and name and residence, ie residence, ie name and seat of the person for whom the transaction is intended; • the manner of execution of the transaction; • information on the source of assets (wealth) and assets, which are or will be the subject of a business relationship or transaction.

If in the process of identification of the client it is not possible to determine all the stated data from the identity document, the missing data shall be obtained from another valid public document submitted by the client.

5.3. Determining and verifying the identity of a legal entity and a company

Determining and verifying the identity of a client who is a legal entity or a company is done by inspecting the original or certified copy of the document from the Central Register of Business Entities (CRPS) or by inspecting the original or certified copy of another appropriate public register, as well as a business or other public register in which a foreign legal entity or company is entered, which is submitted on behalf of the legal entity or company by a representative or an authorized person. The documents on the basis of which the client's identity is established and verified must not be older than three months from the date of issue. The document from the register or other proof of registration must be translated into Montenegrin and certified by the seal of the sworn court interpreter. The identity of a legal entity or company and the prescribed data can be verified by inspecting the CRPS (Website: www.crps.me), or other appropriate public register, as well as a certified copy of the court, business or other public register in which the foreign legal entity is registered. or a company, on which the employee, who performed the inspection, enters the date and time of the inspection, his name and signature. The original or a certified copy of the documents on the basis of which the identification was made, are kept together with other documentation in the client's file. In the process of identifying the client, the following information must be obtained:

Client data to a legal entity or company	
	• name of the legal entity or company • address;

Client data	• the registered office and identification number of the legal entity that establishes the relationship or executes the transaction, or the legal entity for which the business relationship is established or the transaction is executed
Data related to establishing a business relationship	• date of establishment of the business relationship; • The purpose and presumed nature of the business relationship, including information about the client's business.
Data related to the performed transaction	• date and time of transaction execution; • the amount of the transaction and the currency in which the transaction was made; • purpose of the transaction, personal name and residence, ie residence, ie company and registered office of the person for whom the transaction is intended; • the manner of execution of the transaction; • data on the source of assets and funds.
Data on the person representing the client (legal representative, or authorized person, all directors)	• Name; • address of residence or stay; • date and place of birth and tax number of the representative or authorized person, all directors for the legal entity with which the business relationship or transaction is established for the legal entity; • number and type of identity document; • the name of the body that issued the identity document.
Information about the beneficial owner of the client	• Name; • address of residence or stay; • date and place of birth of the beneficial owner of the legal entity; • tax number of the beneficial owner; • number and type of identity document; • the name of the body that issued the identity document.

5.3.1. Determining and verifying the identity of legal representatives of legal entities and companies

Before establishing a business relationship with a legal entity or company, as part of determining and verifying the identity of a client of a legal entity or company, the Company implements measures to identify a representative and all directors for legal entity or company and verifies identity, obtains prescribed information, by inspecting the personal document of the

representative in his presence, as well as by inspecting the personal documents of all directors submitted by the representative.
The employee of the Company conducting the identification is obliged to obtain copies of personal biometric documents of the representative and all directors on which he enters the date and time of the insight, his name and signature.
If the function of legal representative or director in a legal entity or company is performed by a person who has the status of a legal entity, its identification is performed by implementing the prescribed measures in the process of determining and verifying the identity of a legal entity or company with mandatory identification of a natural person who has legal function. The employee of the Company who conducts the identification procedure is obliged to obtain a copy of the personal biometric document of that natural person on which he enters the date, time, his name and signature.
If it is not possible to determine all the prescribed data for representatives and all directors from the obtained personal documents, the missing data shall be obtained from other public documents submitted by the representative, ie the authorized person.

5.3.2. Determining and verifying the identity of the authorized person of the legal entity and the company

If on behalf of the representative and all directors the business relationship of a legal entity or company is established by an authorized person or performs a transaction, the Company determines and verifies the identity of the authorized person of the legal entity or company and obtains the prescribed data. Data on the representative and all directors, on whose behalf the authorized person acts, the employee of the Company conducting the identification obtains by inspecting personal biometric documents and from a written authorization in the original or a certified copy issued by the representative.
The employee conducting the identification is obliged to obtain a copy of the personal biometric document of the authorized person on which he enters the date, time, as well as copies of personal biometric documents of the representative and all directors for legal entity or company on which he enters the date and time and signature. If it is not possible to determine all the prescribed data from the personal documents of the representative or authorized person, the missing data shall be obtained from another public document submitted by the representative or authorized person. Copies of biometric personal documents, original or certified copy of the authority under which it is made identification are kept together with other documents in the file of the client.

5.3.3. Determining and verifying the identity of the beneficial owner of the legal entity and the company

Prior to establishing a business relationship with a legal entity or company, as part of determining and verifying the identity of the client, the Company implements measures to establish and verify the identity of the beneficial owner and obtains the prescribed information on the beneficial owner in a way that ensures client all the way to individuals who are by definition considered the beneficial owner.
According to the definition, the beneficial owner is a natural person who owns or controls the client, or a natural person on whose behalf the transaction is conducted or establishes a business relationship, as well as a natural person who exercises actual control over a legal entity,

company, foreign trust, foreign institution or a similar subject of foreign law. The beneficial owner of a company, ie legal entity is considered to be a natural person who:

1) is, directly or indirectly, the holder of at least 25% of the shares, voting rights or other rights, on
- on the basis of which it participates in the management, ie participates in the capital with more than 25% shares or has
- decisive influence in the management of the property of a company or legal entity;

2) provides funds to a company or legal entity indirectly and on that basis has the right to decisively influence the decision-making of the management body of the company or legal entity when deciding on financing and operations.

If the ownership structure of the client such that it is not possible to identify the beneficial owner according to the definition in point 1, or if it is suspected that a natural person according to the definition set out in item 2 of the beneficial owner, it will be the beneficial owner of a company or entity considered one or more persons in management positions.

The beneficial owner of an association, institution, religious community, artistic organization, chamber, trade union, association of employers, foundation or other business entity is considered to be any natural person authorized to represent or a natural person who has a controlling position in property management.

The beneficial owner of a legal entity, which receives, manages or allocates funds for certain purposes, is a natural person who:

1) directly or indirectly disposes of at least 25% of the property of a legal entity or similar subject of foreign law;
2) at least 25% of the income from the managed property is determined or identifiable as a beneficiary.

Prescribed data on the beneficial owner, determined in the manner described above, are obtained by inspecting the originals or a certified copy of documentation from the Central Registry of Business Entities (hereinafter CRPS) or other appropriate public register as well as by inspecting the court, business or other public register of the foreign legal entity, that must not be older than three months from the date of issue or obtain them by inspecting the CRPS or other public register. If the employee cannot obtain all the data on the beneficial owner of the legal entity or company, he obtains the missing data by inspecting the original or a certified copy of the document or other business documentation provided by the client's representative or authorized person provides a complete and clear insight into the real property and management body of the client. The identity of legal entities in the ownership structure of the client can be verified by inspecting the CRPS (Website: www.crps.me) or other appropriate public register, as well as a certified copy of the court, business or other appropriate public register, in which the foreign legal entity is registered or the company on which the employee who performed the inspection enters the date and time of the inspection, his name and signature. Also, for all natural persons who have been determined as beneficial owners, the employee who conducts the identification of the client, obtains a copy of the personal biometric document of those persons on which he enters the date and time of insight, his name and signature.

Verification of the data on the beneficial owners is carried out by obtaining Beneficial owner declaration as a Company form.

Identification and verification of the identity of the beneficial owner of a legal entity is precisely defined procedure "Know Your Customer".

5.4. Establishing and verifying the identity of a foreign trust to another person, and with him a tie foreign legal entity

In the method of determining and verifying the identity of the foreign trust or another entity, or with it equaled to foreign law apply to the same extent as well as in the identification of a legal person or a company, including the identification and authentication of the authorized agent, or entity. In addition, the process of identification is necessary to identify and verify the identity of the beneficial owner. Foreign beneficial owner of the trust of another person, or to tie them foreign legal entity, it is a natural person who:

- is the founder of a foreign trust, foreign institution or similar subject of foreign law;
- is a trustee of a foreign trust, foreign institution or similar foreign law entity;
- the beneficiary of funds acquired from the assets under management, where future beneficiaries have already been identified or may be identified;
- is a representative of the interests of the recipients of the acquired funds;
- belongs to the category of persons who have an interest in establishing a foreign trust, foreign institution or similar foreign law entity when a legal and natural person benefiting from a foreign trust, foreign institution or similar foreign law entity has yet to be determined;
- is a natural person who otherwise indirectly or directly controls the property of a foreign trust, foreign institution, or similar subject of foreign law.

In the identification procedure, it is obligatory to obtain data that are prescribed as obligatory for a client who is a legal entity or a company.

5.5. Business relationship monitoring and transaction control including re-annual control

Measures to monitor the client's business relationship, including control of transactions, implies the obligation of the Company to perform:

- checking the compliance of the client's business with the nature and purpose of the business relationship;
- control of transactions in accordance with the client's risk profile of money laundering and terrorist financing;
- monitoring and checking the compliance of the client's business with his usual scope of business;
- checking the sources of funds with which the client operates;

- monitoring and regular updating of documents and client data;

Measures to monitor clients' operations are implemented to the extent and dynamics that correspond to the degree of risk determined in the analysis procedure, ie depending on the classification and classification of clients into risk groups, as follows:

- the operations of clients classified in category A (lower risk) are checked every two years;
- the business of clients classified in category B (medium risk) is inspected annually;
- The business operations of clients classified in category C (higher risk) are checked semi-annually.

When executing each individual client transaction, the Company is obliged to minimally determine and understand the following:

- sources of assets and assets that are or will be the subject of a business relationship or transaction;
- date and time of transaction execution;
- the amount of the transaction and the currency in which the transaction will be executed;
- purpose of the transaction (legal and economic logic behind the transaction);
- personal name and residence, i.e. residence, i.e. company and registered office of the person for whom the transaction is intended;
- the manner of execution of the transaction

In order to effectively control transactions, a control system has been established, which includes the implementation of primary and secondary control.

1) Primary control of transactions and accompanying documentation is performed by the employee who is in charge of monitoring the client or is in direct contact with the client. Within primary control, he is obliged to analyze the basis of the transaction from the aspect of compliance with the nature and activity of the client, usual business, economic justification, as well as to determine the source and further destination of funds. The submitted documentation (instruction for payment.) as well as its content must be identical to the purpose of the transaction specified in the transfer order,

2) Secondary control of transactions is performed by the Authorized Person or his deputy. After all performed controls, if the conditions for the transaction are met, the Authorized Person or his deputy, by verifying the order for the transaction, gives approval for the transaction.

At all stages of transaction control, all employees involved in the process are required to apply Indicator Lists to identify suspicious transactions. The identification of a suspicious transaction or client or business relationship is based on the criteria listed in the list of indicators for identifying suspicious transactions and clients. If a transaction or client meets one of the indicators, it does not necessarily mean that it is a suspicious transaction or client, but this fact indicates the need for additional analysis and a broader picture in accordance with the principle of "know your client", to adequately implement measures monitoring the business relationship of that client, which includes monitoring his transactions to determine that those transactions

have a clear purpose and intent, that the origin of the funds has been verified and does not indicate suspicion of money laundering and terrorist financing or any other crime, that there is clear knowledge of the client and his business activities with which he deals, etc.

An employee who is in direct contact with a client, or who in the course of performing the tasks for which he is in charge, suspects that there is a risk of money laundering and terrorist financing in connection with the client or transaction, or if he knows or suspects that the funds represent proceeds of crime or are related to the financing of terrorism, he is obliged to make **an internal report** on it and to submit it to the AML officer or his deputy as soon as possible. The report should contain sufficient data and information about the client and the transaction that enable the AML officer to assess whether the client, i.e. the transaction indicates suspicion of money laundering and terrorist financing. The AML officer analyses the submitted data and information, evaluates, and decides on further action. If the AML officer assesses that the submitted data and information on a potentially suspicious transaction or clients are not relevant for the detection of money laundering and terrorist financing, an official note shall be made stating the facts and reasons indicating that it is not a suspicious transaction or client, as and all transaction data. If the assessment of the AML officer confirms that this is a suspicious transaction, the AML Agency shall be notified in the manner defined in item 7 of this Program.

If it is determined that the transaction meets the criteria to be identified as a complex and unusual transaction, the employee is obliged to apply the measures prescribed in paragraph 5.6.1.3 of the Program.

For clients of legal entities at least once a year, and no later than one year from the date of establishing a business relationship, annual control measures are implemented, which include:

1) obtaining or checking data on the name, address and registered office of the client;
2) obtaining data on the name and residence or domicile of the representative;
3) obtaining data on the beneficial owner;
4) verification of the validity of the power of attorney;
5) updating of the PEP Form of all identified natural persons in the legal entity (representative, director, authorized person, beneficial owner)

In the procedure of re-annual control of foreign legal entities, as well as legal entities based in Montenegro, if the share of foreign capital in that legal entity is at least 25%, the prescribed data are obtained by inspecting the original or certified copy of documentation from CRPS or other appropriate public register. , which must not be older than three months from the date of issue, ie by inspecting the CRPS or other appropriate public register. If it is not possible to obtain all the prescribed data by inspecting the documentation, these data are obtained from the original or a certified copy of documents and other business documentation submitted by the representative or authorized person of the legal entity, or directly from the written statement of the client's representative.

In the procedure of annual control of resident legal entities, the prescribed data are obtained and verified by inspecting the CRPS or other appropriate public register and the time of inspection, their name and signature. If, based on the performed inspection, changes in the data contained in the Company's records are determined, the employee is obliged to obtain the original or a certified copy of the documentation from the CRPS or other appropriate public register without delay.

For resident legal entities, the original or a certified copy of the documentation from the CRPS or other appropriate public register shall be submitted no later than two years from the establishment of the business relationship / implementation of the annual control.

For all clients, natural persons, an updated PEP Form is obtained no later than one year from the day of establishing the business relationship.

5.6. Special forms of checking and monitoring clients' business

5.6.1. In-depth customer verification, business relationship monitoring and transaction control

Measures of in-depth customer verification, business relationship monitoring and transaction control are mandatory in the following cases:

- when concluding a business relationship or when conducting one or more related occasional transactions in the amount of EUR 15,000 and more, with a client who is a politically exposed person, or a client whose representative, director, authorized person, , as well as the beneficial owner politically exposed person;
- when concluding a correspondent relationship with a bank or other financial institution, an institution based outside the European Union, or not on the list of countries applying measures at the level of standards in the field of prevention of money laundering and terrorist financing equivalent to those applied in the European Union or more ;
- in complex and unusual transactions;
- in the case of electronic money transfer;
- application of new technology;
- when a higher level of money laundering and terrorist financing risk has been identified in accordance with the national risk assessment
- when concluding a business relationship or conducting transactions with a client from a high-risk third country
- as in all other cases where, based on the risk factors identified in the Analysis, it is determined that there is a higher risk of money laundering and terrorist financing

5.6.1.1. Correspondent relations

In the context of the above, a "correspondent account" is an account opened for a foreign bank and / or other financial institution to which the Company receives deposits from a bank and / or other financial institution or makes payments or other payments on behalf of a foreign bank or other financial transactions related to such a foreign bank.

Foreign banks are foreign banks without a physical presence in any country. "Foreign bank" is any bank organized under foreign law or an agency, branch or office of a bank located outside Montenegro.

The decision on the establishment of a correspondent relationship is made by the Chief Executive Officer after a thorough quality check of the financial institution with which the establishment of a correspondent relationship is planned, and which is carried out by the AML officer.

Correspondent relationship is a relationship that arises by opening an account of a foreign bank or other similar financial institution with the Company in order to provide services by the Company. Standard measures when establishing a correspondent relationship include:

- Implementation of measures to establish and verify the identity of a foreign bank or other similar institution, its legal representatives, directors, authorized persons and beneficial owner in the manner described in item 5.3. of this Program;
- Identification of members of the Board of Directors of a foreign bank or other similar institution by obtaining a copy of the personal biometric documents of those persons on which he enters the date, time, his name and signature;
- Obtaining a copy of the license of a bank or other similar institution, analysing the validity of the license by checking the date of issue, time of validity of the license, name and seat of the competent authority that issued the license, as well as analysis of license authorizations;
- Obtaining a copy of the statute of the bank or other similar institution and analysis of the statute including the content of the powers given to its directors and their proxies;
- Obtaining certified signatures of representatives;
- Obtaining signature specimens;
- Analysis of the relationship with the immediate superior group (if any);
- Obtaining and analysing the Wolfsberg questionnaire;
- Checking the available information in Bankers Almanac.

When establishing a correspondent relationship with a foreign bank or other credit or other similar financial institution based outside the European Union or not on the list of countries applying international standards in the field of prevention of money laundering and terrorist financing that are at the level of European Union standards or higher, as well as in all cases where it is assessed that there is a high risk of money laundering and terrorist financing, the Company applies in-depth measures, which in addition to the above standard measures include obtaining data, information and documentation:

- on internal procedures carried out to detect and prevent money laundering and terrorist financing, in particular client verification procedures, identification of beneficial owners, communication of suspicious transactions and clients, competent authorities, record keeping, internal controls and other procedures, which is a party to a bank or other credit institution determined in connection with the prevention and detection of money laundering and terrorist financing;
- on the assessment of internal control over the implementation of measures to prevent money laundering and terrorist financing at the correspondent bank or other credit institution;
- legal or institutional arrangements in the field of detection and prevention of money laundering and terrorist financing applied in another state in which it has its registered office, ie in which a foreign bank or other credit institution is registered;

- a written statement issued by a foreign bank or other credit institution in the country in which it is domiciled or registered that, in accordance with the laws of that country, it is obliged to apply appropriate regulations in the field of detecting and preventing money laundering and terrorist financing, including information on whether it is under investigation for money laundering and terrorist financing or whether measures have been taken against it by the competent authorities;
- a written statement that a foreign bank or other financial institution does not operate as a quasi-bank or quasi-financial institution;
- a written statement that a foreign bank or other financial institution has not established, ie does not establish business relations or perform transactions with quasi-banks or other financial institutions;
- a written statement that the foreign bank or other financial institution, in relation to the intermediary account, has confirmed the identity and performed a continuous procedure with the client who has direct access to the correspondent's account and is able to provide appropriate data from the procedure with the client.

5.6.1.2. Politically exposed persons

Before establishing a business relationship with a client or executing a transaction, the Company is obliged to determine whether the client is a politically exposed person ("PEP"), as well as to determine whether any of the identified individuals is a legal entity or company, trust or to another person (representative, directors, authorized person, and beneficial owner) PEP .
In order to determine whether a person is a politically exposed person ("PEP"), the Company conducts the following procedures:

a) Obtains a form to be completed by the client when establishing a business relationship ("PEP Form"). For the client legal entity, the PEP Form is filled in by all identified natural persons in the legal entity (representative, directors, authorized person, and beneficial owner)
b) Queries the database of politically exposed persons World Check Pep List which is integrated into the AML / FT tool.

When it is determined that the client is PEP or that one of the natural persons in a legal entity or company, trust or other person (agent, director, authorized person, as well as the beneficial owner) is PEP, an employee who proposes to establish a business relationship, is obliged to apply measures of in-depth verification of the client, monitoring of the business relationship and control of transactions, which include the following:

- Determining the source of property (wealth) and the source of the client's funds from personal and other documents submitted by the client. If the prescribed data cannot be obtained from the submitted documents, the data are obtained from a written statement of the client;
- obtaining the written consent of the Chief Executive Officer before establishing a business relationship with the client, or if a business relationship with the client has already been established, obtain the written consent of the Chief Executive Officer to continue the business relationship;
- after establishing a business relationship, pays special attention to transactions and other business activities performed by PEP with the Company, as well as a legal entity or company, trust or other person whose representative, director, authorized person, as well

as actual the owner identified as a PEP specifically considering the source of the asset and the source (origin) of the funds, as well as the purpose and intent of the transaction and compliance with its normal business.

The Company maintains a List of Politically Exposed Persons (the "List"), which contains data on clients of natural persons identified as PEP, as well as data on clients of legal entities in which they are a representative, director, authorized person, , as well as beneficial owner PEP. The list is available to all employees who are in direct contact with clients in order to ensure the implementation of in-depth verification measures and for those clients who were not PEP at the time of establishing the business relationship.
The list contains the following information:

- for the natural person: name, unique citizens identity number or passport number, address of residence or stay (street, house number, place and country), information on the function of the politically exposed person, ie the degree of kinship or cooperation with the person in a prominent public position, date of establishment business relationship, name and surname of the employee in charge of the client, date of termination of political exposure and name and surname of the employee who made the change of data;
- for the client legal entity: name of the client, identification number, registered office address, date of establishment of the employee in charge of the client, date of termination of political exposure and name and surname of the employee who changed the data.

The AML officer or his deputy is responsible for updating the List. The List is updated by updating the PEP Form no later than 12 months from the date of establishing a business relationship with the client.
If in any of the above ways it is determined that a client is a natural person or a representative, director, authorized person, and beneficial owners of a client of a legal entity received the status of PEP Authorized person is obliged to include these persons on the List and notify the employee in charge of the client to obtain from the client an updated PEP Form, the consent of the Chief Executive Officer to continue the business relationship and implement other measures related to doing business with politically exposed persons.
Also, if it is determined that the obligation to treat the client as a PEP has ceased (due to the expiration of 12 months from the date of termination of public office), the Authorized Person is obliged to exclude that person from the List, as well as his family members and associates. obtain an updated PEP Form for the client and re-classify the risk according to the Risk Analysis.

5.6.1.3. Complex and unusual transactions

Complex and unusual transactions are those transactions that are characterized by complexity and unusually high amounts, unusual manner of execution, value or connection of transactions that have no economic justification or visible legal purpose, or are not consistent or disproportionate to the usual or expected business of the client. circumstances related to the status or other characteristics of the client. Due to the characteristics of complex and unusual transactions, the distinction between suspicious transactions and unusual transactions is specific, because a transaction characterized by complexity and unusually high amount and manner of execution often has elements that could indicate suspicion of money laundering.

An employee who has established a business relationship with a client and who monitors his business, knows best to what extent and in what way he operates, that is, what his regular business and changes in the account are, so he can notice when the client's business and activities begin to deviate from usual, in order to pay special attention to it and perform an analysis and determine the reasons for that deviation. When evaluating a transaction and determining its nature, the employee should answer the following questions, which define the basic criteria for determining a complex and unusual transaction:

1. Is the transaction unusually high for this client?
2. Does the client perform the same or similar transaction more often than would be normal?
3. Is the type of transaction unusual, having in mind the client's previous business?

Based on the given answers, supported by valid evidence, employees will be able to get an idea of whether it is an individual case of deviation from normal business, or it is a case, that is, elements of money laundering. In addition to all IT tools and procedures, a good analysis requires a good knowledge of the client regarding:

- type, business profile and structure of the client,
- geographical origin of the client,
- the nature of the business relationship, product or transaction,
- previous experience in doing business with the client,
- status and ownership structure of the client,
- the purpose of concluding a business relationship or executing a business transaction,
- client information obtained from publicly available databases and other data and information,
- other information that may indicate that the transaction is unusual.

If the employee identifies a certain transaction as complex and unusual, he is obliged to apply in-depth measures:

- collects and verifies additional data on the client's activity and updates the identification data on the client and the beneficial owner of the client,
- collect and verify additional information on the nature of the business relationship and information on the purpose of the announced or performed transaction, and
- Collect and verify additional data on the client's assets, origin and source of funds.

All complex and unusual transactions, the employee is obliged to analyse and to record the results of the analysis in writing so that the results of the analysis are available at the request of theAML Agency;. If the analysis determines that there are no grounds for suspicion of money laundering or terrorist financing, the employee who monitors the client's business, within its competences, gives consent for the transaction and submits information to the AML Officer that the transaction is analysed as unusual. The AML officer keeps records of all approved complex and unusual transactions centrally.
If, based on the conducted analysis, it is determined that there is a suspicion of money laundering or terrorist financing, the employee is obliged to act in the manner described in item 5.5. Program.

5.6.1.4. Electronic transfer of funds

Electronic transfer of funds means telecommunication transfer of orders, issued by the ordering party, ie the payer of funds in written or electronic form, for payment in the country or abroad.
The Company, in addition to standard measures of knowledge and monitoring of business and transaction control, collects accurate and complete data on the payer and enters them in the form or message that accompanies the electronic transfer of funds sent or received in the currency subject to electronic transfer. while moving through the payment chain.
The Company, as an intermediary or recipient of funds, is obliged to refuse the transfer of funds if the data on the payer are incomplete and / or to request that the data on the payer be supplemented as soon as possible.

5.6.1.5. New technologies

The application of new technologies such as internet trading, the use of ATMs, etc., also increases the risk of money laundering and terrorist financing. In order to adequately manage the risk arising from the provision of internet trading services and the use of other new technologies, it is envisaged that new technologies can be used only by clients with whom the Company has established business relations and to whom all measures envisaged by this Program have been applied. During transactions of Internet service users, the identification of the signatory, the authenticity of the signed electronic document, the integrity of electronic messages or documents to exclude the possibility of forgery, as well as denial of responsibility for their content is provided by a unique, secret password for identification - mobile token.

The company is obliged to closely monitor the business activities of users of Internet financial services that are the result of the application of other new technologies, analyses transactions that pose a higher risk of money laundering and terrorist financing.
Professional services in the field of information systems and security, within their competencies and responsibilities, provide additional measures that eliminate risks and prevent the misuse of new technologies for money laundering and terrorist financing and provide systems that enable the safe use of new technologies.
When introducing new technologies in the provision of existing or new products and services, the Organizational Part of the Company that initiated the process is obliged to obtain from the AMl officer an assessment of the impact of these changes on the Company's exposure to money laundering and terrorist financing . In addition to the impact assessment, AML officer is obliged to propose measures in accordance with the results of the assessment in order to reduce the risk of money laundering and terrorist financing. The introduction of new technologies in the provision of existing or new products and services must not be carried out without the adoption of the proposed measures.

5.6.1.6. Clients from high-risk third countries

The term high-risk third countries means countries that do not apply or do not sufficiently apply measures to prevent and detect money laundering or terrorist financing in accordance with the FATF lists. A list of high-risk third countries is given in the Risk Analysis. The AML officer or his deputy is responsible for updating the list.
For clients who come from high-risk third countries when entering into a business relationship or executing a transaction, in addition to standard measures of checking and monitoring the client's business, additional measures of in-depth checking and monitoring of the client and transaction control are taken, which include collecting additional information conducting these checks:

- collecting and verifying additional data on the client's business activity and updating identification data on the client and the beneficial owner;
- collecting and verifying additional data on the nature of the business relationship and data on the purpose of the announced or completed transaction;
- collecting and verifying additional data on assets, the origin of assets and the source of funds
- Information about the identity of the client or the actual owner of the client, or the ownership structure and control of the client, in order for the Company to be confident in an adequate understanding of the risks associated with the business relationship. This includes collecting and evaluating information about the reputation of the client or beneficial owner, as well as assessing any negative allegations regarding the client or beneficial owner, eg: information about past and existing business activities of the client or beneficial owner; searching for media allegations that negatively impair that client's reputation, information about family members, or close business partners.
- Increasing the quality of information about the presumed nature of the business relationship in order to determine that the nature and purpose of the business relationship are legal and so that the Company can more adequately assess the risk profile of the client. This includes collecting data and information on the number, significance or dynamics of expected transactions per account, to enable discrepancies to be identified that may indicate suspicion; the reason why the customer seeks a particular product or service, especially when it is unclear why the customer's needs cannot be better met in another way or in another jurisdiction; destination of funds; the nature of the business of the client or beneficial owner, to enable the client to more easily understand the announced nature of the business relationship.
- Improving the quality of information gathered for the purpose of applying in-depth client verification measures to verify the identity of the client or the beneficial owner of the client, including verifying that the client's assets and assets used in the business relationship do not originate from criminal activity. in accordance with the Company's knowledge of the client and the nature of the business relationship
- increasing the frequency of checks to ensure that the Company is still able to manage the risk associated with an individual business relationship or to conclude that the business relationship no longer corresponds to the risk profile of the obligor, and to better identify transactions that require additional analyses including the following: a) increased frequency of checks and monitoring of business relationships to determine whether the client's risk profile has changed and whether that risk can continue to be managed; b) more frequent monitoring of the business relationship to ensure that any changes in the client's risk profiles are identified, assessed and, if necessary, the necessary measures are taken or more frequent and in-depth analysis of transactions is carried out to identify any unusual or unexpected transactions raise suspicion of the risk of money laundering and terrorist financing.

To enter into a business relationship with clients from high risk third countries, employees of the Company, which proposes establishing a business relationship with a client, he must obtain the written consent of the Chief Executive Officer.

5.7. Determining and verifying the identity of the client based on a qualified electronic confirmation of the client

The identity of a client who is a natural person can also be determined on the basis of a qualified electronic certificate of the client issued by the certification service provider in accordance with the regulations.
The Company accepts for identification qualified electronic certificates issued by providers of electronic trust services based in Montenegro that are registered in the register of qualified providers of electronic trust services in Montenegro and in the European Union
The Company accepts for identification of qualified electronic certificates issued by providers of electronic trust services based in another country that is not part of EU have the same legal right as a qualified electronic certificates issued in Montenegro, fulfilling the legal requirements prescribed by the Law on Electronic Identification and Electronic Signature and if:

1) the certification service provider for electronic transactions meets the requirements prescribed by law for the issuance of qualified certificates and is registered in the register of qualified providers of electronic trust services in Montenegro or is registered in a Member State of the European Union;
2) is a qualified provider of electronic trust services registered in the register of qualified providers of electronic trust services in Montenegro or registered in a Member State of the European Union guarantees such a qualified certificate;
3) are in accordance with an international agreement concluded between Montenegro and another state or international organization;
4) are in accordance with an international agreement concluded between the European Union and a state that is not a member of the European Union or an international organization;
5) the provider of electronic trust services meets the conditions established by the regulations of the European Union for the issuance of qualified certificates and if it is registered in a Member State of the European Union;

In case the Client decides to complete the process of concluding the contract with the client and making the transfer electronically, the contract documentation will be made on a permanent data carrier in electronic form (electronic documents) and signed by a qualified electronic certificate of the Client and the Company regulations governing the field of electronic document and electronic signature.
In the case referred to in Article 14 paragraph 2 and 3 of the Law on Prevention of Money Laundering and Terrorist Financing, when the client's identity is established on the basis of a qualified electronic certificate of the client, data that cannot be obtained from a qualified electronic certificate are obtained from a copy of identity document submitted by the client in writing or electronically.
When the Client and / or the Client's legal representative and authorized person are absent during identification (eg execution of transactions using the trading platform), the Company requires the use of a qualified digital certificate and password to verify identity to sign documents and execute transactions.
In order to securely identify the client who is a user of the Company's services, the Company may use, with a qualified electronic signature, various methods of identification, including PINs, passwords, smart cards, biometrics, etc.
After the initial identification of the Client using a qualified electronic signature and / or handwritten signature of the documentation, the Client identifies himself by accessing the Company's services by means of Identification, Authorization and Signature as follows:

- identification with the User name and password: individual Services of the Company are accessed by entering a combination of the unique User Name received by the User from the Company and the password created by the User,
- identification by Username and PIN: individual Services of the Company are accessed by entering a combination of a unique Username that the Client received from the Company and the PIN of the user,
- PIN identification: certain services of the Company are accessed by entering a unique PIN created by the User;
- identification with a Qualified electronic certificate: certain services are accessed using the medium on which the Qualified electronic certificate of the User is located and by entering the PIN,

The Company is obliged to apply appropriate technological procedures and equipment that ensure the protection of these documents, in accordance with the law governing archives, regulations on office operations and international standards in the field of document management.
In the identification procedure, the Company obtains data on the client from a qualified electronic certificate, which it records and keeps in its database on the basis of Article 78 and 79 of the Law on Prevention of Money Laundering and Terrorist Financing.
The Client is obliged to keep the resources and data for the formation of a qualified electronic signature from unauthorized access and use and bear any responsibility for misuse and unauthorized use by third parties and / or loss, with the obligation to immediately request the revocation of his qualified certificate in all cases of loss or damage to the means or data for forming an electronic signature. Clients are obliged to provide the Company without delay, immediately after the change, with all necessary data and information on changes that affect or may affect the accuracy of establishing its identity.
When an operation or Transaction requires the signature of the User, the Company and the User agree and accept that the use of the appropriate means of identification, authorization and signature, when requested, has the value of a qualified electronic signature, which allows its identification and proves its consent for remote (electronic) signing contractual documents for products or services offered by the Company, if applicable.
The User is obliged to keep secret the Means of identification, authorization and signature (all passwords, etc.) that he uses to access the services of the Company and all possible damage caused by non-compliance with this provision shall be borne by the Client.
The Company archives all messages related to the Transaction that the Client delivers to any of the available communication channels (including, but not limited to e-mail, SMS, voice record of telephone conversation, logs from web servers, etc.) in accordance with the prescribed deadlines.
The Client is obliged to take into account the Statements / Reports and notifications received from the Company and is obliged to review them, with the obligation to notify the Company of any disagreement and / or correction and / or observed errors.
The Company will provide and continuously prove that all measures are taken to identify and verify the identity of the client through e-KYC, and only measures that are safe and effective.
The Company will adopt an appropriate combination of authentication factors when establishing measures to verify a client's identity through e-KYC. The strength and combination of authentication factors will be proportionate to the risks associated with the incorrect identification of a particular product or service, as decided by the Company's Board of Directors.

When using the electronic identification system, the Company will always take into account three basic factors of authentication:

- something that the client owns (eg ID card, registered mobile number, utility bill number),
- A fact that the client knows (e.g. PIN, personal information) i
- The facts the client requires is (e.g. biometric characteristics).

The Company will perform e-KYC where identification and verification in a way that the decision to verify the client is made by a representative of the Company, intermediary or agent / representative of the Company, with the exclusive use of qualified electronic signature and additional electronic means such as video calls using mobile devices and the like.
The Company will consider situations where there is a potential for a higher risk of misidentification and establish the necessary safeguards to address this risk.

Addressing existing vulnerabilities

The Company will continuously identify and address potential vulnerabilities in the e-KYC solution.
Actions to address potential vulnerabilities include conducting reviews of e-KYC solutions and, where possible, providing periodic feedback to technology vendors to improve the efficiency of the underlying technology used to identify and verify customers.

5.8. Determining and verifying the identity of the client through a third party

Acceptance of identification by a third party (financial institution)
Pursuant to Article 22 of the Law on Prevention of Money Laundering and Terrorist Financing, an authorized person in the Company does not have to identify a client in one of the above ways in case the identification and determination of the purpose and intended nature of the transaction or business relationship a financial institution that complies with the rules and takes sufficient measures to prevent money laundering that are comparable to those that exist in the Company and that the Company has at the same time provided information, including copies of relevant documents to identify the client, purpose and purpose of the transaction or business the relationship and identity of the beneficial owner from the financial institution that performed the identification or determined the relevant data.
The Company will not accept information about the identification of the client, information about the purpose and intended nature of the transaction or business relationship or the determination of the beneficial owner if there are doubts about the accuracy or completeness of such information.
The following financial institutions are among those from which the Company may accept identification:

1) a bank and other credit institution and a branch of a foreign bank;
2) an investment fund management company, a branch of a foreign investment fund management company and a company from the Member States of the European Union that is authorized to directly perform investment fund management activities on the territory of Montenegro;
3) pension fund management company;
4) authorized participant in the securities market and branches of a foreign legal entity in Montenegro who performs the following activities:

- intermediation in the purchase and sale of securities on the client's order in his own name, and for someone else's account with the payment of a commission (brokerage);

- management of the portfolio of securities belonging to another person (investment manager's activities) and legal entities licensed by the Capital Market Commission to perform custody operations, except for banks;

5) life insurance companies and branches of foreign life insurance companies;
6) brokerage companies, and representation companies and entrepreneurs-representatives in insurance in the part related to life insurance;
7) an equivalent person with a seat in a state of the European Union or another state that applies measures in the field of prevention of money laundering and terrorist financing at least at the level of measures determined by this Law.

A third party who, in accordance with Article 22 of the Law on Prevention of Money Laundering and Terrorist Financing, establishes and verifies the identity of the client is obliged to submit to the Company the obtained data and documentation on the client.
If the Company assesses that there is doubt in the credibility of the determination and verification of the client's identity by a third party or in the veracity of the obtained data on the client, it is obliged to directly determine and verify the client's identity.
The company may not accept the implemented measures referred to in Article 8, paragraph 1, item 1, 2 and 3 of the Law on Prevention of Money Laundering and Terrorist Financing, by a third party if that person has established and verified the identity of the client without his presence.
When the Company uses third parties for identification purposes, this person participates in fulfilling, in the name and on behalf of the Company, the duty of care imposed on it by the Law on Prevention of Money Laundering and Terrorist Financing.
Entrusting the affairs of the Company referred to in Article 8, paragraph 1, item 1,2 and 3 of the Law on Prevention of Money Laundering and Terrorist Financing, the company performs the decision of the Board of Directors respecting the following principles:

- entrusting the implementation of measures referred to in Article 8, paragraph 1, item 1, 2 and 3 of this Law does not diminish the liability of the Company to a third party to fully fulfil its legal and regulatory obligations, nor to transfer that responsibility to a third party;

- entrusting the implementation of measures referred to in Article 8, paragraph 1, item 1, 2 and 3 of this Law shall not diminish the decision-making powers, on SPNFT especially on the adoption of procedures to prevent money laundering and trafficking in human beings that must be respected by a third party, the decision to enter into a business relationship or assign a risk profile to a client. suspicious transactions are reported or the Anti-Money Laundering Authority is notified of the asset freeze, etc,

- The Company will monitor the implementation of tasks performed by a third party to detect any deficiencies, and will immediately take appropriate and effective remedial action in the event of third party deficiencies and, where applicable, terminate the contract for the transfer of these tasks without delay. in the event of serious omissions, without such termination being jeopardizing the continuity of the tasks assigned to the third party;

Entrusting the implementation of measures referred to in Article 8, paragraph 1, item 1, 2 and 3 of the Law on Prevention of Money Laundering and Terrorist Financing may include continuous supervision aimed at detecting atypical transactions, analysing these transactions in accordance

with internal procedures, collecting all additional information and preparing an opinion based on this analysis regarding (un) suspicious the nature of the transaction under consideration.
Entrusting the implementation of measures referred to in Article 8, paragraph 1, item 1, 2 and 3 of the Law on Prevention of Money Laundering and Terrorist Financing, the Company will, as a rule, perform to third parties that meet the requirements of Article 22 of the Law on Prevention of Money Laundering and Terrorist Financing, and which belong to the same group these functions in different entities of the group (eg centralization of certain IT tools in the parent company).
Entrusting the implementation of measures referred to in Article 8, paragraph 1, item 1, 2 and 3 of the Law on Prevention of Money Laundering and Financing of Terrorists within the Group are subject to the same requirements as for external services. When using the inner group engagement of external associates to perform Client identification tasks, the Company should take the measures necessary to identify and manage any conflict of interest that may arise from such a trust agreement.
The transfer of client identification tasks from Article 8, paragraphs 1, 2 and 3 of the Law on Prevention of Money Laundering and Terrorist Financing, requires that the following conditions be met:

1. The transfer decision should be preceded by a documented analysis to identify the risks associated with that transfer, including the risks associated with the use of new technologies in this context, to define the measures to be applied for management and to reduce these risks.
2. The transfer decision should be properly reasoned in the light of the objectives pursued, clearly indicating whether it was taken in accordance with the principle of proportionality and / or whether it aims to ensure optimal distribution of funds throughout the group to which the Company belongs.
3. It is the obligation of the Authorized Person to Prevent Money Laundering and Terrorist Financing to;

   - monitoring the performance of service providers (third parties) to ensure that they effectively enable the Company to comply with all its legal and regulatory obligations regarding SPNFT;
   - reporting on the transfer of external affairs to the Board of Directors (or, where applicable, senior management) or whenever circumstances require, special reporting so that all necessary remedial measures are implemented as soon as possible.
   - Keeps a register of concluded contracts entrusting the performance of these tasks referred to in Article 8, paragraphs 1, 2 and 3 of the Law on Prevention of Money Laundering and Terrorist Financing;
   - Maintains a precise list of tasks assigned to a third party and the procedures to be performed by a third party in performing those tasks, and arrangements for regular monitoring of completeness, timeliness and quality of service provided by a third party are established in writing (service level agreement); The service level agreement explicitly states whether the third party is authorized to use sub-outsourcing and, if so, specifies the exact arrangements for them;
   - The Company shall ensure that the contract for the transfer of these operations contains the necessary explicit provisions to prevent this agreement from interfering with the control tasks of the Company's internal audit, compliance and AML functions;

5.9. Using a third party as an "independent party business introducer"

For the purpose of establishing the client's identity, a distinction is made between two types of situations in which different identification rules apply:

- use of a third party to whom the Company entrusts the implementation of measures referred to in Article 8, paragraph 1, item 1, 2 and 3 of the Law on Prevention of Money Laundering to a third party who meets the conditions prescribed by Article 22 of this Law;

- the use of a "third-party business introducer" in such cases the independent business editor himself is subject to the obligation of in-depth analysis prescribed by the Law on Prevention of Money Laundering and Terrorist Financing and fulfils them in accordance with his own procedures.

The use of a third-party business introducer differs from the use of a third party in that it does not act primarily in the name and on behalf of the Company on the basis of a mandate (transfer of authority to perform this business).) which he received from the Society. Since ("third-party business introducer") itself is subject to identical or equivalent obligations of due diligence, in accordance with the Law on Prevention of Money Laundering and Terrorist Financing or comparable law of another state, it primarily fulfils the obligations of due diligence of its clients according to its own procedures, independent of the Company. It then submits the result of its own due diligence obligations to the Company to which it represents its client, enabling that financial institution to take that result into account in order to meet its own due diligence obligations and avoiding, as far as possible, the same due diligence obligations.
The Company may rely on a "third-party business introducer" in order to meet the following general obligations:

- obligations of identification and verification of identity;
- the obligation to determine the characteristics of the client and the purpose and nature of the business relationship;
- obligation to update information;
- Obligations regarding the collection and verification of information necessary to fulfill the obligation of in-depth analysis regarding occasional transactions and transactions performed during the business relationship.

During the implementation of the contract on the execution of transactions from Article 8, paragraph 1, items 1, 2 and 3 of the Law on Prevention of Money Laundering, the Company will check whether the legal and regulatory provisions and supervision imposed on third parties meet the equivalence requirements of Article 22 of the Law on Prevention of Money Laundering and Terrorist Financing. .
In accordance with Article 3 of the Law on Prevention of Money Laundering and Terrorist Financing, the Company will, when relying on a function relying on an independent third-party business introducer, request that the latter immediately provide information on the identity of clients and, if necessary, its agents and beneficial owners, as well as the characteristics of the client and the purpose and intended nature of the business relationship, arising from the due diligence requirements carried out by a third-party business introducer in accordance with law or equivalent foreign law to which it is subject.

When entrusting the business, the Company will take appropriate measures to enable the independent representative of the company to send them immediately and at the first request a copy of supporting documentation or reliable sources of information used to verify the identity of the client and, if necessary, its agents and beneficial owners.
Obligatory entities may accept the results of an in-depth customer due diligence obligation carried out by an independent third-party business introducer located in an EEA country or in a third country, even when the data or supporting documents used to identify or identity verification differs from those required by Montenegrin regulations.

5.10. Simplified customer verification, business relationship monitoring and transaction control

Simplified measures for establishing and verifying the identity of the client, monitoring the business relationship and control of transactions are applied in cases where based on risk factors, according to the Risk Analysis, it is determined that there is a lower risk of money laundering and financing in relation to the client, business relationship terrorism. The collected data is checked and stored in accordance with this Program.
The stated data are obtained by inspecting the originals or certified copies of the documentation from the CRPS (Central Register of Business Entities) or other appropriate public register, which is submitted by the client, or by direct inspection. If the prescribed data cannot be obtained in the described manner, the missing data shall be obtained from the original or certified copies of documents and other business documentation submitted by the client or from a written statement by the client's representative or authorized person. The documentation must not be older than three months from the date of issue.

6. Measures to prevent terrorist financing

Unlike money laundering, terrorist financing has different characteristics, and therefore risk assessment of terrorist financing requires more risk assessment factors, as well as more complex methods to determine the existence of terrorist financing.

The nature of sources of terrorist financing can vary depending on the type of terrorist organization, given that the funds used to finance terrorist activities can come from both legal and illegal sources. When sources of funding for terrorist activities arise from criminal activities, then a money laundering risk assessment approach is also applicable to terrorist financing. Given that transactions related to terrorist financing are usually realized in small amounts, these transactions, given the amount of them, through the application of an approach based on risk assessment of money laundering, are considered low-risk transactions, makes it very difficult to determine terrorist financing.
In cases where the sources of financing terrorist activities come from legal sources, then it is more difficult to determine that the legally acquired funds are used for terrorist purposes. In this regard, some activities for the preparation of terrorist acts may be undisguised, such as the purchase of necessary materials or payment for certain services.
The issue of determining terrorist financing is complex, and the obligation of employees is especially related to the reporting of suspicious transactions that may be related to terrorist financing. In this regard, it is extremely important to monitor cash transactions and transactions

to countries, for which the relevant international organizations or bodies have determined to finance or assist terrorist activities.
Measures implemented by the Company in the process of managing the risk of terrorist financing include:

- monitoring and updating the lists of organizations and persons associated with terrorists or terrorist organizations on the basis of notifications from the competent institutions;
- checks, to the extent objectively possible, whether funds from legal sources or transactions, to a greater or lesser extent, are directed to support terrorist activities;
- application of internal and external procedures, guidelines and indicators for detection and identification of suspicious clients and transactions related to terrorist financing, including the obligation to urgently report to the AML Agency;
- revealing the actual identity of the participant in the transaction and the purpose of the transaction, especially when the purpose of the transfer and the sender or recipient are not clearly stated;
- cases when the client's account unexpectedly empties the account;
- cases of money laundering in which money is received or sent electronically, and are accompanied by unusual aspects, such as the amount, the country to which the money is sent, the country of the ordering party, the type of currency, etc .;
- non-profit and humanitarian organizations, especially if they perform activities for which they are not registered, if the source of funds is not clear or if the organization receives funds from unusual and suspicious sources or donors.

7. Reporting

The authorized person prepares the following types of reports:
1) Quarterly report: The authorized person is obliged to prepare a quarterly report on activities to prevent money laundering and terrorist financing. The report shall be submitted to the Board of Directors for adoption, no later than the end of the month following the end of the quarter to which the report relates. After approval by the Board of Directors, the report can be submitted to the AML Agency or Capital Market Authority in three days after receipt of the request quarterly report, as a minimum, contains data on:

- results of performed checks and tests of the Program with a proposal of measures to be implemented, methods of implementation;
- the number and nature of requests and orders received from the AML Agency;
- complex and unusual transactions;
- suspicious transactions;
- the total number of suspended transactions;
- the total number of requests for continuous monitoring of customer accounts.
- performed impact assessments on the risk of money laundering and terrorist financing before all important changes in business processes such as, introduction of new products, new practices, including new distribution channels, introduction of new technology for new and existing products, services or organizational changes; proposing risk mitigation measures;
- Newly discovered ways and techniques of money laundering with a long list of measures for their recognition and detection;

- problem-solving activities observed in the application of procedures and practices for identifying suspicious transactions;
- results of training of employees with information on the date of training, topics presented and names of persons who attended the training;
- proposing measures to improve policies and procedures for detecting and preventing suspicious transactions
- findings and recommendations of the Capital Market Authority control with the status of implementation,
- findings and recommendations of internal controls with the status of implementation.

2) The AML officer is obliged to prepare the Annual Report on activities to prevent money laundering and terrorist financing, no later than the end of March of the current business year for the previous year. This report can be submitted to the AML Agency or Capital Market Authority in three days after receipt of the request.

3) Semi-annual and Annual report for the Capital Market Commission: AML officer prepares a report twice a year on activities to prevent money laundering and terrorist financing for the first half of the year and for the whole year
4) Report on suspicious transactions: The AML officer is obliged to inform the AML Agency about the suspicious transaction without delay in the prescribed manner before its execution, ie to submit data and information on the reasons that indicate suspicion of money laundering and terrorist financing or any other criminal offence, that is, the reasons that clearly and unambiguously indicate that it is a suspicious transaction, client or business relationship and state the indicators on the basis of which the assessment was made that it is a suspicious transaction, client or business relationship.
5) Cash Transaction Report-Upon receipt of data and information on cash transactions, the AML Person prepares a Cash Transaction Report containing all data on transactions of EUR 15,000 and above. The report is prepared in the form defined by the Rulebook on submission of data on cash, suspicious and other transactions. The report on cash transactions is submitted to the AML Agnecy, without delay, and no later than within three working days from the day of the transaction. The mentioned report is submitted via official web sites of AML Agnecy. In case the report cannot be submitted via the web portal due to technical deficiencies, the AML Person or his Deputy are obliged to submit the report and all accompanying documentation to the AML Agency in paper form by the end of the working day.

The AML Agency is notified in the form of Form O1 which is in Annex 1 of this Program (if the application is made electronically on the web portal: www.uprava-spn.co.me) or, if this is not possible, by personal delivery. If the AML person is not able to inform the AML Agency about the suspicious transaction in the prescribed manner before its execution due to the nature of the transaction or other justified reasons, he is obliged to subsequently inform the AML Agency, but not later than the next business day. AML officer is obliged to submit an explanation and state the reasons for which he could not objectively inform the AML Agency within the prescribed period The report submitted to the AML Agency on a suspicious transaction, must be supported by documentation and the reasons for which they are so characterized. The Company may disclose this information to the AML Agency by telephone, but is obliged to submit this information in writing, no later than the next business day from the day of notification. For a transaction, client or business relationship suspected of money laundering and terrorist

financing, the Company is obliged to refuses to execute the transaction or to inform the AMl Agency before its execution of the reasons for suspicion, so that the AMl Agency would be able to prevent the execution of that transaction or to block it, in accordance with its competencies. Further execution of the transaction reported to the AMl Agency as suspicious is suspended, until the AML Agency sends the Company the appropriate information, ie instruction or binding order to act.

In the event that subsequent checks during the monitoring of the client's business for a particular transaction is found to be suspicious, information about the transaction is submitted to the AML Agency in writing as previously described, immediately after learning that it is a suspicious transaction, or no later than the next working day knowledge.

The AML officer is obliged, upon individual requests of the AML Agency, to submit data, information and documentation without delay and in the form specified in the request, and no later than eight days from the receipt of the request, unless otherwise stated in the request. For the purpose of timely response to the requests of the AML Agency, the AML officer is obliged to request from the head of organizational units to inspect the records and documentation in their possession and to submit the requested data, information and documentation in the required form. The heads of the organizational units, in whose possession the documentation is located, are obliged to submit the documentation and the specification of the submitted documentation to the AML officer within the stipulated deadline. The heads of the organizational units, in whose possession the documentation is located, are responsible for the accuracy and timely delivery of the documentation and information to the AML officer.

After receiving the documentation, the AML officer prepares the answer to the inquiry and forwards it to the AML Agency. The answer is submitted via the web portal (www.uprava-spn.co.me) or, if that is not possible, by personal delivery. The answer to the request is also submitted in the case when a certain person or persons from the request are not in the records and databases of the Company.

The AML Agency may, by written order or, in urgent cases, orally, issue a temporary suspension order if it assesses that the client or transaction is subject to suspicion of money laundering or terrorist financing and related predicate offences or terrorist financing. The temporary suspension of the execution of the transaction may last for a maximum of 72 hours from the day from the moment of the temporary suspension of the execution of the transaction. If this deadline falls on non-working days, this deadline can be extended by an order for an additional 48 hours. If the Management Board, after the expiration of the period of 72 hours, does not inform the Company about further actions towards the client or the transaction, the Company may execute the transaction in question and inform the Management Board about it.

The AML Agency may, in writing, require the Company to continuously monitor the financial operations of the client, in connection with which there are grounds for suspicion of money laundering or terrorist financing and related predicate offences or terrorist financing or other persons for whom may conclude that it has cooperated or participated in transactions or transactions for which there is a basis for suspicion of money laundering and terrorist financing and related predicate offences or terrorist financing and set a deadline within which it is obliged to inform and submit the requested information.

The Company is obliged to submit the stated data to the Aml Agency before the execution of the transaction or the conclusion of the transaction and to state in the announcement the estimate of the deadline within which the transaction or transaction should be performed.

This measure may last for a maximum of three months from the receipt of the request and may be extended for a maximum of three months, counting from the day of receipt of the request.

The AML officer is responsible for acting upon the requests and orders of the AML Agency.

8. Keeping and content of records

The Company is obliged to keep records of following:
1) Records of data on clients, business relations, accounts and transactions (. The records are kept in a way that provides for the reconstruction of individual transactions (including amounts and currency) that could be used as evidence in the process of detecting criminal activities of clients and includes the following data:

- name, address, registered office and identification number of the legal entity that establishes the business relationship or executes the transaction, or the legal entity for which the business relationship is established or the transaction is performed;
- name, address of residence, ie residence, date, place of birth and tax number of the representative or authorized person, who for a legal entity, foreign trust, other person, or an equal subject of foreign law concludes a business relationship or executes a transaction, number and type of personal documents and the name of the body that issued the identity document;
- name, address of permanent or temporary residence, date, place of birth and tax number of all directors of the legal entity, foreign trust, other person, ie equal subject of foreign law, number and type of identity document and name of the body that issued the identity document;
- name, address of permanent or temporary residence, date, place of birth and tax number of authorized persons of the legal entity, foreign trust, other person, or a subject of foreign law equated with it, number and type of identity document and name of the issuing authority identity document;
- name, address of residence or domicile, date and place of birth and tax number of the natural person, , performing the activity, who establishes a business relationship or executes a transaction, or natural person for whom a business relationship is established or performed transaction and number, type and name of the body that issued the identity document;
- the purpose and presumed nature of the business relationship, including information about the client's business;
- the date of establishing a business relationship,;
- registration number of the identification number of each client account;
- date and time of transaction execution;
- the amount of the transaction and the currency in which the transaction was made;
- purpose of the transaction
- the manner of execution of the transaction;
- information on the source of assets and assets that are or will be the subject of a business relationship or transaction;
- reasons for suspicion of money laundering and related predicate offences or terrorist financing;
- name, address of residence or stay and date and place of birth of the beneficial owner of the legal entity, ie information on the category of person in whose interest the establishment and operation of the legal entity or similar legal entity of foreign law is;

- name or name of the foreign trust, other person, or subject of foreign law equated with him, address of residence, ie residence, date and place of birth and tax number of the person referred to in Article 18 of this Law.

2) records of data on complex and unusual transactions;
3) records of orders on temporary suspension of the transaction;
4) records of requests for continuous monitoring of the client's financial operations;
5) records on training of employees and professional training of persons responsible for the implementation of activities to prevent money laundering. Records on professional training of employees contain data on persons who attended the training and evidence of their attendance at the training, as well as signed statements of employees on the initial training, pursuant to item 10 of this Program.
6) records with data on persons and transactions in connection with which there is a basis for suspicion that it is money laundering and terrorist financing. The data are entered in chronological order, neatly and up-to-date. The data are entered in such a way that the incorrectly entered word or part of the text is crossed out in such a way that the previous text remains legible, and the new entry is entered legibly above the crossed out text.
7) records on access of supervisory bodies to data, information and documentation for which there is a prohibition of disclosure. The AML officer is obliged to inform the AML Agencyin writing about any access of the competent authority, no later than within three working days from the performed inspection. Records of access by supervisory authorities shall include the following information:

- name of the supervisory body;
- the name of the authorized official who performed the inspection;
- reason for conducting the inspection;
- date and time of data access.

9. Data protection and storage

The Company and its employees are bound to data, information and documentation obtained in implementing the measures and tasks related to the management of risk of money laundering and terrorist financing are used only for the purposes for which they were obtained and ensure their preservation and protection.
Employees, including employees with access to data records and documentation obtained in the implementation of measures and tasks related to money laundering and terrorist financing risk management, must not disclose to a client or a third party that:

- the transaction or client has been reported or will be reported to the AML Agency on suspicion of money laundering and terrorist financing;
- the AML Agency temporarily suspended the transaction, ie gave instructions to the Bank in this regard;
- the AML Agency required regular monitoring of the client's operations;
- A client or third party has been or could be investigated for money laundering or terrorist financing.

The prohibition on disclosure of the specified data does not apply to:

- data, information and documentation that are necessary for establishing the facts in criminal proceedings and if the submission of such data in writing is requested or ordered by the competent court or prosecutor's office;

- information required by the Capital Market Authority.

In cases where the Company rejects the request to establish a business relationship, the employee may not explain to the client the reasons for inadmissibility and refusal to enter into a business relationship. In that sense, the notification must be oral and must not hurt or discriminate against the potential client. If the request for establishing a business relationship is rejected, an appropriate level of discretion is required so as not to harm the potential client and the Company's image.
Information on data submitted to the AML Agency, notifications on suspicious transactions, requests and orders of the AML Agency, as well as all other data, information and documentation exchanged with the AML Agency shall be marked with the appropriate security classification designation and may not be disclosed to third parties. Electronic forms of requests and orders of the Management Board and responses of the Company are stored on the computer of the AML officer Documentation on transactions or persons in connection with which there is a basis for suspicion of money laundering and terrorist financing, the AML officer keeps in a metal safe separate from other documentation. Data whose degree of secrecy has been determined in accordance with the Law on Data Secrecy shall be kept:

- 30 years (information marked "TOP SECRET");
- 15 years (information marked "SECRET");
- 5 years (classified information "CONFIDENTIAL");
- 2 years (classified information "INTERNAL").

Data obtained through the implementation of measures related to money laundering risk management and terrorist financing, copies of identity documents, other documents and documentation, as well as written authorizations, other supporting documentation, data on the identification number of each client account, data and documentation on electronic money transfer, documentation on business correspondence and reports are kept for ten years after the termination of the business relationship, the completed transaction and access to the safe deposit box.
Data and accompanying documentation on the AML officer and deputy , professional training of employees and implementation of internal control measures shall be kept for ten years from the dismissal of the AML officer and deputy , ie performed professional training and internal control.

10. Education and training

Professional and quality performance of tasks in the field of detection and prevention of money laundering and terrorist financing, implies continuous education and training of employees. The AML officer is obliged to take care of the regular training and education of all employees who perform tasks in the field of detecting and preventing money laundering and terrorist financing. Professional training and education from the previous paragraph refers to acquainting employees with the provisions of the Law on Anti-money laundering and terrorist finansing and bylaws for its implementation, internal acts, indicators for identifying suspicious clients and transactions, literature on detecting and preventing money laundering and terrorist financing, as well as other topics. The training is conducted on two levels:

1. Each employee is provided with a set of external and internal regulations, which he is obliged to study and then sign a statement that he has read and understood the

regulations (initial training). Initial training is performed whenever the internal acts of the Company are harmonized with the applicable legislation, as well as for newly employed persons within the deadlines prescribed by this act;
2. conducting trainings in the form of lectures with working material in accordance with the Training Program (regular training).

For the needs of regular training of employees, the AML officer is obliged to prepare the Program of professional training and advanced training of employees who perform the tasks of detecting and preventing money laundering and terrorist financing, no later than the end of the first quarter of the business year.
The AML officer is obliged to train employees at least once a year in the previously announced time, in the form of lectures (PowerPoint presentations) and simulation of regular business activities and communication with clients. All employees whose tasks in any way relate to the implementation of measures related to the prevention of money laundering and terrorist financing, must be included in the Program for professional development program.
Education must be tailored to the special needs of employees according to the specifics of the work they perform: employees who are in direct contact with clients, employees who participate in the process of establishing a business relationship.
Special attention must be paid to new employees, who must be acquainted with the basic measures taken at the Bank to detect and prevent money laundering and terrorist financing. The AML officer is obliged to provide initial training in the field of AML and FT to every new employee in the Company, depending on his / her job, no later than 15 days from entering the employment relationship. Regular training will be conducted in accordance with the deadline set in the Vocational Training and Development Program.
The AML officer checks the knowledge and training of employees at least once a year. The results of the performed checks are kept within the deadlines prescribed for data storage and accompanying documentation on professional training (item 8 of the Program).
The AML officer shall inform the Board of Directors and the Management Board on an annual basis about the results of the training of employees with information on the date of the training, topics presented and the names of the persons who attended the training.

The training of the AML officer and his deputy is constant and is organized by competent institutions and external consultants, and refers to the issue of money laundering and terrorist financing, as well as training in all economic and legal segments that can improve the quality of work of employees. The training refers to:

- getting to know and monitoring legal and regulatory changes
- introduction to new methodologies for preventing money laundering and terrorist financing;
- training in recognizing new forms, techniques and trends related to money laundering and terrorist financing.

Evidence of the training of the AML officer and his deputy is kept in their personal files.
The AML officer is obliged to inform all employees without delay about any changes in regulations (laws, bylaws, guidelines, etc.). The AML officer is obliged to harmonize the internal acts with the changes as soon as possible, and no later than the expiration of the legal deadline for harmonization.

11. Internal control

By conducting internal control and audit, the Company regularly monitors the application of internal acts and assesses their adequacy and compliance with legal regulations. Internal control is carried out:

- control by the AML officer
- control by the Department for monitoring compliance with regulations;
- Control by Internal Audit.

The AML officer periodically, and at least quarterly, by the method of accidental cause or in another appropriate manner, checks and tests the application of the Program for the Prevention of Money Laundering and adopted internal acts. The results of the performed checks with the proposal of measures form an integral part of the Quarterly Report of the AML officer. In addition to the occasional control of the implementation of the Program, the AML officer conducts regular control by giving consent when establishing a business relationship with the client, as well as during the implementation of individual transactions.
The Department for Monitoring Compliance with Regulations, in accordance with the annual plan, conducts an audit of activities to prevent money laundering and terrorist financing in order to assess the compliance of operations with the Law and bylaws. The report on the performed control is submitted for approval to the Board of Directors.
In accordance with the annual work plan, based on risk assessment, the Internal Audit Department checks the compliance of the Company's operations with legal regulations and internal acts, evaluates the system of internal controls in work processes, gives orders and recommendations for eliminating identified irregularities and improving the existing system. The audit report shall be submitted to the Board of Directors for approval.

12. Lists of sanctions and embargoes, lists of FATF and other restrictions

Competences and responsibilities of employees in the application of restrictive measures pursuant to the Law on International Restrictive Measures, types of restrictive measures, procedure for application and abolition of restrictive measures, technological support for implementation of measures and manual control, keeping records and reporting to competent state and company bodies are prescribed by the Implementing Procedure. restrictive measures.
The Company uses the AML / FT tool in order to verify the data on persons entering or having established a relationship with the Company in relation to the data contained in the sanctions lists.

13. Others

In resolving all issues and defining actions related to the prevention of money laundering and terrorist financing that are not regulated in detail by this Program, the Law and other regulations related to the operations of banks, as well as instructions of competent state bodies, will be applied.

The AML Authorised Person is responsible for the interpretation of the Program.

The program is reviewed at least once a year. The AML officer is obliged to make adjustments as soon as possible in case of changes in regulations governing the prevention of money

laundering and terrorist financing, as well as due to strategic, organizational and functional changes in the structure of the Company.

The program enters into force on the day of its adoption.

Chairman of the Board of Directors

_____

Finveo
The Capital Plaza, Cetinjska 11
81000 Podgorica, Montenegro
T +382 20 436 698
info@finveo.mn • www.finveo.com

14. APPENDIX

INTERNAL LIST OF INDICATORS OF SUSPICIOUS TRANSACTIONS

1. The Client provides the Company with unusual or suspicious identification documents that cannot be easily verified or contradict other statements or documents submitted by the Client as well as other available information about the Client. This indicator can be applied to account opening and post-account interaction.
2. The Client hesitates or refuses to provide the Company with complete information that is necessary for in-depth analysis of the client. as required by the Company's procedures, which may include information regarding the nature and purpose of the client's business, previous financial relationships, anticipated account activity, company location and, if applicable, company employees and directors.
3. The client refuses to identify a legitimate source of funds, provides information that is inaccurate or misleading
4. The client resides, operates regularly or occasionally in a jurisdiction known as a bank secrecy sanctuary, tax haven, high-risk geographical location (eg known as a narcotics jurisdiction, known to have ineffective AML / Anti-system terrorist financing) or conflict zones, including those with an identified threat of terrorism.
5. The client has difficulty describing the nature of his business or has no general knowledge of his industry.
6. Other financial services companies have rejected or terminated the customer as a client.
7. The client's legal or postal address is linked to several other accounts or companies that are not linked.
8. A client is an investment firm that does not want to provide information about controllers and clients.
9. The client is publicly known or the company is aware that criminal, civil or regulatory proceedings are being conducted against him or her for a crime, corruption or misuse of public funds, or is known to associate with such persons. Sources for this information may include news, the Internet, or a search of commercial databases.
10. The Client's background is questionable or differs from expectations based on business activities.
11. The client maintains multiple accounts or maintains accounts in the names of family members or legal entities, for no apparent business or other purpose.
12. An account is opened by a politically exposed person (PEL), in particular in relation to one or more additional risk factors, such as an account opened by a quasi-company or under the supervision of a PEL. The PEL is from a country that the FATF has identified has strategic shortcomings in the money laundering regime or the PEL is from a country known to have a high level of corruption.
13. The account shall be opened by a non-profit organization providing services in geographical locations known to be at greater risk of being an active terrorist threat.
14. An account shall be opened in the name of a legal entity involved in the activities of an association, organization or foundation whose objectives are related to the claims or claims of a known terrorist entity.
15. A client is a legal entity - a fast growing company whose business is suspicious. From the documentation submitted by the client, it is not easy to recognize how he generates income.

16. An account is opened for the alleged joint stock company, which may hold limited securities of insiders in companies that have secured those securities as collateral and then settled the loan obligations, after which the securities are sold in an unregistered manner.
17. An account is opened on behalf of a foreign financial institution, such as an offshore bank or broker-dealer, that sells shares in an unregistered manner on behalf of buyers.
18. An account has been opened for a foreign financial institution with no apparent business purpose.
19. The client opens a new account and deposits financial instruments that are a large block of securities that are rarely traded or have a low price.
20. The client has a form for depositing financial instruments or a form for the delivery of shares electronically, the current sale of shares, and then transfers the proceeds from the sale.
21. The Client deposits or transfers shares that:
    - have recently been issued or represent a large percentage of floating securities;
    - give a reference to the name of the company or client that has been changed or does not match the name on the account;
    - they were issued by the grenade company;
    - they were issued by a company that has no obvious business, income or products;
    - they were issued by a company whose application with the competent regulator is not current, incomplete or does not exist at all;
    - issued by a company that has undergone several recent name changes or business combinations or recapitalisations;
    - they were issued by a company that was the subject of a previous suspension of trading; or
    - is issued by a company whose employees or insiders have a history of regulatory or criminal violations or are associated with multiple issuers of cheap shares.
22. Data from the register of deposited shares are not in accordance with the date when the buyer acquired securities, the nature of the transaction in which the securities were acquired, the history of shares or the volume of trading in shares.
23. A client with limited or no other assets receives transfers of large quantities of unlisted securities to the companies.
24. The explanation or documents of the client, which prove that he has acquired shares, do not make sense or change after examination by the Company or other parties.
25. The Client deposits physical securities or delivers shares electronically, and within a short period of time requests that the shares be recorded in multiple accounts that appear unrelated or that the shares be sold or otherwise transferred.
26. Seemingly unrelated clients open accounts at or about the same time, deposit the same cheap collateral and subsequently liquidate it in a way that suggests coordination.
27. The client engages, for no apparent reason, in transactions involving certain types of securities, such as small shares, and bearer bonds, which, although legitimate, have been used in connection with fraudulent schemes and money laundering activities. (Such transactions may justify further detailed analysis to ensure the legitimacy of the client's activities.)
28. Investor demand has risen sharply, along with rising prices, cheap or cheap securities.
29. The Client's activity represents a significant share in the daily volume of trading in securities that are rarely traded or have low prices
30. A client buys and sells securities with no apparent purpose or circumstances that appear unusual.
31. Individuals known throughout the industry as promoters of financial instruments sell securities through brokers.

32. The buyer accumulates inventory in small increments during the trading day to increase the price.
33. Engaging a client in pre-arranged or other non-competitive securities trading, including laundering or cross-trading, for no apparent business purpose.
34. A client attempts to influence the closing price of a share by executing a buy or sell order at or near market close.
35. A client engages in transactions suspected of being associated with cyber breach of client accounts, including potentially unauthorized disbursements or trade.
36. The client is often included in the order of placing orders on one side of the market, usually within an existing national best bid or offer (NBBO), followed by entering orders on the other side of the market that execute against other market participants. who joined the market in the improved NBBO (activity indicating "false representation")
37. The client is often faced with placing multiple border orders on one side of the market at different price levels, followed by entering orders that are executed on the opposite side of the market, and the customer cancels the original limit orders (
38. Two or more unrelated client accounts in the Company suddenly and simultaneously trade in illiquid or cheap securities.
39. A client makes a large purchase or sale of a security, or an option on a security, immediately prior to the issuance of a news item or a significant announcement affecting the price of a security.
40. The client deposits money frequently and in large amounts, insists on trading only in cash equivalents or seeks an exemption from the company's policies and procedures relating to the deposit of cash and cash equivalents.
41. A client “structures” deposits, withdrawals, or purchases of monetary instruments below a certain amount to avoid reporting or record keeping, and may directly state that it is trying to avoid initiating a reporting obligation or evading tax authorities.
42. The client seemingly divides the funds into smaller transfers to avoid drawing attention to the larger transfer of funds. Smaller transfers of funds do not appear to be based on wage cycles or other legitimate regular deposit and withdrawal strategies.
43. The Client's account shows a number of currencies, money orders (especially sequentially numbered money orders) or cashier's check transactions, which are combined into significant amounts without obvious business or legal purpose.
44. The client often changes the details of the bank account
45. The client deposits funds, followed by a request that the money be paid or transferred to a third party or other company, without any obvious business purpose.
46. Bank transfers are made in small amounts in an apparent effort to avoid initiating requests for identification or reporting.
47. Electronic transfer takes place to or from financial secret havens, tax havens, high-risk geographical locations or conflict zones, including those with a determined presence of terrorism.
48. The buyer is involved in transactions involving the exchange of foreign exchange that are briefly accompanied by foreign exchange transfers to places of special importance (eg countries designated by national authorities, such as the FATF, as non-cooperative countries and territories).
49. The parties to the transaction (eg initiator or beneficiary) are from countries known to support terrorist activities and organizations.
50. Electronic transfers or payments are made to unrelated third parties (foreign or domestic) or from them or where the name or account number of the user or remittance is not specified.

51. There is an activity of electronic transfer that is inexplicable, repetitive, unusually large, shows unusual patterns or has no obvious business purpose.
52. A securities account is used for payments or outgoing bank transfers with little or no securities activity (ie the account appears to be used as a depository account or transfer channel, which could be used for business operational needs) .
53. Funds are transferred to financial or depository institutions other than those from which the funds were initially received, especially when different countries are involved.
54. A foreign company receives payments outside the area of its client base.
55. Transactions involving round or full dollar amounts with the intention of including payment for goods or services are common.
56. The Buyer opens and closes accounts with the Company and then reopens a new account with the Company, each time with new ownership information.
57. The client invests the product without worrying about the investment goal or performance.

INTERNAL LIST OF INDICATORS FOR FINANCING TERRORISM

1. Beneficiaries of telegraphic transfers are nationals of countries associated with terrorist activities;
2. When an employee determines on the basis of a passport that the client has traveled to blacklisted countries or countries where ISIL manages certain territories, and tries to make cash payments without submitting a customs declaration of money transfer across the state border and proof of origin;
3. If the employee doubts the validity of the identification document;
4. If a large number of foreign inflows in smaller amounts by a larger number of natural persons without a clear basis is recorded on an account that has not been active for a long time.

LIST OF GENERAL INDICATORS

1. The client brings in a large amount of cash with the intention of making transactions.
2. The client's business transactions are not in line with his income and assets.
3. The client gives vague explanations about the source of income or cash used in business transactions.
4. There is information that the client may be involved in illegal activities.
5. The client requests to pay in installments in order to avoid paying the amount of cash subject to reporting in accordance with the Law on Prevention of Money Laundering and Terrorist Financing.
6. The client requests that the report on the cash transaction not be made or refuses to perform the transaction after learning that making the report is mandatory.
7. The transaction performed by the client is not in accordance with his usual business practice.
8. The client wants to buy property or do business on behalf of someone else (acquaintance or relative other than his or her spouse).
9. The client does not want his name to appear on any document that would link him to a given business transaction.
10. The client gives an inadequate explanation why he changes the names of the person he uses in connection with the transaction at the last moment.

11. The client negotiates to perform the business at the market price or the price higher than the requested one, but requires that the documents state a lower value, paying the difference in price "below the counter".
12. The client pays an advance in a large amount of cash, while the rest is financed from an unusual source or a bank in an area with low income tax rates or no income tax (hereinafter: offshore destination).
13. The client inquires about unusual payment methods.
14. Transfers of small amounts of cash involving the same persons through other alternative money transfer systems have become more frequent.
15. Significant transfers of funds to accounts on which there were no transactions (inactive accounts) which were immediately followed by the withdrawal of funds, ie. by withdrawing cash.
16. Learning from reliable sources (including the media or other open data sources) that indicate that the client is involved in some illegal activities.
17. A new or prospective client is known as a person for whom there is information that he is involved in illegal activities or is a person known for criminal activities.
18. Cash deposit where the same payment order is attached as proof of origin, and the amount of deposited cash is significantly higher than the amount indicated on the payment order.
19. Payment of obligations is often made by the client through bonds.

OFFICIAL LIST OF INDICATORS OF SUSPICIOUS TRANSACTIONS FOR CAPITAL MARKET

1. Frequent trading of financial instruments when the purchase is made by depositing cash in dedicated accounts, and soon after the sale of financial instruments below cost.
2. Contracted block trade in shares, especially when unknown or newly formed companies appear as buyers, especially those coming from offshore destinations.
3. The client (legal entity) has a complex structure that makes it difficult to determine or allows to hide the identity of the beneficial owners.
4. The client performs an activity that is marked as high risk in accordance with the National Assessment of Risk of Money Laundering and Terrorist Financing.
5. In addressing the investment company that provides investment services, the investor (natural person) acts exclusively through a proxy.
6. The client operates through intermediaries such as investment managers, advisors, lawyers or accountants, in order to make it difficult or avoidful to establish their own identity.
7. Purchase of financial instruments performed with funds deposited in several accounts in different banks, especially if funds are deposited that are slightly below the amount prescribed for reporting, ie reporting in accordance with the Law on Prevention of Money Laundering and Terrorist Financing.
8. The client invests in securities of large and very successful companies ("blue-chip stocks"), or in very profitable securities with good returns, and does not show interest in the results or suddenly and without reason to sell them.
9. The client has a bad reputation, his illegal activities from the past are known or his past cannot be verified.
10. The client frequently changes investment firms in an effort to conceal capital market activities and financial condition or has multiple accounts with different investment firms.
11. Trading in shares in stock exchange and over-the-counter operations that were the subject of a pledge on the basis of approved loans to shareholders - the so-called. dragging stocks through the stock market.

12. The client shows interest in purchasing financial instruments for large amounts without special analysis or advice from an investment adviser, and such a transaction has no obvious economic justification.
13. The client insists on investing in financial instruments that do not fit his profile, even when he is suggested to invest in more favorable financial instruments.
14. The client comes from a country which, based on data from relevant international organizations and the organizational unit of the state administration body responsible for internal affairs that performs activities related to the prevention of money laundering and terrorist financing (hereinafter: financial intelligence unit), does not apply standards in the field of prevention of money laundering and terrorist financing or trading is carried out on stock exchanges from that country.
15. When planning a transaction, the client intends to deposit the assets in several accounts (with the same bank, but different branches or with different banks), and to transfer the sum of payments, which is a significant amount, to countries known for drug production and / or trafficking. to countries that do not apply or do not sufficiently apply measures to prevent and detect money laundering and terrorist financing.
16. A client operates through a capital market investment service provider outside its place of residence, even though there is a capital market investment service provider in that client's place of residence.
17. The client uses companies from different countries to open numerous accounts.
18. Transactions with a country considered non-cooperative by the FATF or establishing business relationships with clients residing in that country.
19. A non-resident client uses domestic accounts for trading on foreign stock exchanges through foreign branches with different controls and identification practices within measures to prevent money laundering and terrorist financing.
20. The client requires the investment firm to transfer securities to another person without monetary compensation, on the basis of a gift contract or other similar basis (FOP transactions - free of payment).
21. Transfer of shares in the form of gifts to unrelated persons, gift of shares by employees for the benefit of legal entity managers, transfer of shares that have legal or out-of-court settlements between persons in larger amounts as legal basis, activation of pledge for non-fulfillment of approved loans, entry of shares for the purpose of establishing legal entities, agreements on status changes of the joint stock company, as well as transfer of securities between persons in the consortium.
22. The client often (several times in one month) buys or sells shares in amounts slightly below the amount prescribed for reporting or reporting in accordance with the Law on Prevention of Money Laundering and Terrorist Financing.
23. A client who has not been active before, suddenly performs transactions on the capital market in a large volume and value.
24. Client trading patterns suggest that he may have insider information.
25. The client (legal entity) has no visible business, income or products, which may indicate that it is a "quasi-company (shell company)" used for trading in financial instruments.
26. A client is an individual known for or associated with predicate offenses such as insider trading, market manipulation or securities fraud.
27. Trading in financial instruments in cases where the owners of financial instruments authorize third parties to manage their ownership and cash accounts and where there are "related" monetary transactions in trading in financial instruments between the owner and authorized persons.

28. Trading in financial instruments for the benefit of legal entities from offshore destinations that use custody services provided by authorized credit institutions or investment firms.
29. Transfer of funds to the accounts of financial institutions or banks other than those specified when establishing a business relationship, especially when those accounts are in other countries.
30. Accounts for financial instruments opened with capital market investment service providers are rarely used to trade in these instruments.
31. The client makes an unusual request for protection of privacy, especially in relation to data related to his identity, activity, property or business.
32. The client offers to pay a higher fee to the provider of investment services in the capital market in order to keep certain information about himself confidential.
33. The client is reluctant to provide information to the capital market investment service provider on the nature and purpose of its business, previous financial relationships, expected activities, managers or business location.
34. The client refuses to disclose the origin of funds or provides false, misleading or substantially inaccurate information to a capital market investment service provider.
35. The client withdraws the order in order to avoid identification, after being informed of the obligation to identify himself in accordance with the Law on Prevention of Money Laundering and Terrorist Financing.
36. The client does not show interest in the commission, other costs and risks of the transaction.
37. The client tries to create an image of the actual trade in financial instruments, and performs an apparent (fictitious or simulated) trade in these financial instruments.
38. A client is a newly established domestic legal entity whose founding capital is low and invests significant amounts of cash in trading in financial instruments.
39. Trading in financial instruments where there is a deviation from price fluctuations - offers, which deviate enormously from the zone of fluctuation.
40. A client makes significant purchases or sales of securities immediately prior to the publication of news that affect the price of those securities (eg, the client has never invested in equity securities but does so at an opportune time).
41. It is known that a client has friends or family members who work for the issuer of securities.
42. A client who trades in low-value securities suddenly takes a significant share in certain securities and makes a significant profit from them.
43. The client participates in pre-agreed or non-competitive securities trading (WASH or CROSS trading in illiquid securities or low price securities).
44. Securities that have been illiquid for a long period of time are traded suddenly, through two or more unrelated accounts in an investment firm or in several investment firms.
45. Transactions of one or more related parties solely so that one party makes a profit and the other a loss.
46. Transactions in which one party buys financial instruments at a high price and then sells them with significant losses to the other party. Also, this can be an indicator of market manipulation.
47. There is no evidence of transactions, ie transactions are without a clear basis.
48. The client inquires about how quickly he could close the account without explaining why he intends to do so or giving dubious explanations about the reasons for closing the account.

INDICATORS FOR TERRORISM FINANCING

1. The ordering party or the recipient of the transaction is connected with the states that are known for providing support to terrorist acts and organizations or areas in which terrorist acts take place.
2. The client uses bogus companies for terrorist financing activities, including quasi-companies.
3. Persons marked on the consolidated list of the Sanctions Committee on the basis of Resolution 1267 of the United Nations Security Council, the black list of the European Union, ie the Office of Foreign Assets Control (OFAC) list, etc. appear in the transaction, ie business relationship. or persons suspected of being connected with persons on the said lists.
4. According to the media, the account holder is associated with a well-known terrorist organization or is associated with terrorist acts, terrorist financing, violent extremism, fundamentalism, or religious radicalism.
5. The client uses the accounts of intermediaries, trusts, family members or a third party.
6. The client provides forged or false identification documents.
7. A non-profit organization does not use funds in accordance with the purpose of its establishment.
8. A larger number of persons authorized on the same account of natural persons, ie non-profit organizations and frequent changes of authorized persons on the account.
9. Transfers funds to locations that do not have a clear business relationship with the client or the state that does not apply or does not sufficiently apply measures to prevent and detect money laundering or terrorist financing.
10. The client engages in commercial financial transactions involving the movement of funds to or from locations where measures to prevent and detect money laundering and terrorist financing are not applied or insufficiently applied when there do not appear to be logical business reasons for doing business with those locations.
11. The transaction deviates from normal account activities.
12. Deposits are in amounts less than prescribed by law in order to avoid the obligation to report and disclose.
13. Large number of cash payments and withdrawals
14. The transaction has no business or economic justification.
15. Unusual cash transaction in bank accounts in another country.
16. Using a large number of accounts opened with a bank in another country.
17. It is suspected that the client is performing transactions on the instructions of another person
18. There is information that a client who has a bad reputation or who has doubts about the sources of funds, uses virtual currencies in their business, e.g. Bitcoin or Litecoin either uses alternative payment channels (eg havala, hundi), in order to avoid regular financial channels.
19. Simultaneous use of cards, in different countries, issued to the same client.
20. A person is associated in the media with terrorist acts, terrorist financing, violent extremism and fundamentalism, or religious radicalism.
21. Transactions for which the employees, based on the experience, knowledge and information at their disposal, have assessed that they are not in accordance with the usual activities of the client.
22. Transactions of a non-profit organization are realized in such a way as to avoid the obligation to report on transactions.
23. Requests for transfer of non-profit organization funds are accompanied by unclear explanations.

24. The programs and activities of a non-profit organization are vaguely explained to supervisory or regulatory bodies.
25. It has been established that the activities of a non-profit organization support individuals or organizations whose identity corresponds to the identity of the entities marked on the lists for the application of restrictive measures.
26. A non-profit organization transfers funds or conducts activities in areas known for the presence of terrorist units.
27. Records of non-profit organizations are kept in areas known for the presence of terrorists.
28. Representatives of non-profit organizations often travel to areas known for the presence of terrorist units.
29. A nonprofit organization has unreported activities, programs, or partners.
30. A non-profit organization uses an unusually complex financial network for its business.
31. A non-profit organization avoids the reporting obligation prescribed by the Law on the Prevention of Money Laundering and Terrorist Financing.
32. The expenses of a non-profit organization are not in line with its programs and activities.
33. A non-profit organization is unable to account for all of its funds used.
34. A non-profit organization is unable to calculate the origin of its income.
35. A non-profit organization has inconsistencies in its accounting and / or mandatory reporting with prescribed anti-money laundering and anti-terrorist financing regulations.
36. A non-profit organization has non-transparent management or decision-making structures.
37. Representatives of a non-profit organization or the non-profit organization itself use falsified or contradictory documentation.

Finveo
The Capital Plaza, Cetinjska 11
81000 Podgorica, Montenegro
T +382 20 436 698
info@finveo.mn • www.finveo.com