

Approved by
"APRICOT CAPITAL"
closed joint stock company
Chief Executive Officer
Vachik Gevorgyan



10 January, 2024

"APRICOT CAPITAL"
CLOSED JOINT STOCK COMPANY
COMBATING MONEY LAUNDERING AND
TERRORISM FINANCING
REGULATION

Yerevan 2024

CHAPTER 1. GENERAL PROVISIONS

1.1 "Regulations on Combating Money Laundering and Terrorist Financing" (hereinafter "Regulations") of "APRICOT CAPITAL" closed joint stock company (hereinafter referred to as the "Company") include measures to combat and prevent money laundering, terrorist financing, and the proliferation of weapons of mass destruction. The measures and procedures shall be implemented by the Company.

1.2 This Regulation is an internal legal act and is adopted in accordance with Article 23 of Law N'e H0-80-N of the Republic of Armenia from May 26, 2008, "On Combating Money Laundering and Terrorist Financing", in accordance with the decision of the Republic of Armenia Board of the Central Bank N'e 279-N from October 7, 2014 , "On minimum requirements to reporting entities in the field of preventing money laundering and terrorism financing", based on the Law of the Republic of Armenia "On Normative Legal Acts". The Regulation was developed in accordance with the requirements of RA legislation and legal acts of the RA Central Bank.

1.3 The requirements of this Regulation should apply to all employees of the Company.

1.4 The main concepts used in this Regulation are as follows:

- **"Senior Management"** - an employee of the Company or a body authorized to make decisions and take actions on behalf of the Company on issues related to preventing money laundering and terrorism financing and financing of the proliferation of weapons of mass destruction. Responsible employees of the Internal Compliance Unit.
- **"ML/TF"** - money laundering and terrorism financing.
- **"FPWMD"** - financing the proliferation of weapons of mass destruction.
- **"Authorized Body"** - Central Bank of the Republic of Armenia.
- **"Law"** - Law NQ H0-80-N of the Republic of Armenia from May 26, 2008, "On Combating Money Laundering and Terrorist Financing".
- **"Responsible employee of the Internal Compliance Unit/ICU"** - an employee of the Company performing the functions of preventing money laundering, terrorism financing and financing of the proliferation of weapons of mass destruction.
- **"Risk"** - circumstance indicating the danger of ML/TF and its probability, which can be characterized by countries or geographical locations, types of customers, types of Transactions or Business Relationships, types of services or other criteria defined by the Authorized Body.
- **"High Risk Criterion"**- a criterion established by the Law, normative legal acts of the Authorized Body and this Regulation, which indicates a high probability of money laundering or terrorist financing.
- **"Business Relationship"**- recurrent services provided to the customer by the Company, which are not limited to one or several occasional transactions.
- **"Transaction"** - a transaction concluded between the Company and the Client or the Authorized Person, as well as between the Client or the Authorized Person and another

person, a transaction that is carried out through the Company or is subject to the Company's monitoring.

- **"Occasional Transaction"**- a Transaction which does not give rise to obligations for the provision of periodic services and (or) does not imply the establishment of a business relationship.
- **"Linking Occasional Transactions"** - occasional Transactions of a uniform nature involving the same party, which are executed within 24 hours.
- **"Other party to the Transaction"** - another participant in the Transaction carried out by the Client, who provides the funds or to whom the assets resulting from the Transaction are addressed.
- **"Suspension of a transaction or business relationship"** - temporary blocking of actual and legal movement of property subject to a suspicious transaction and (or) business relationship.
- **"Rejection of a transaction or business relationship"** - failure to perform actions intended for the execution of a transaction or for establishment of a business relationship.
- **"The termination of a business or a business relationship"** - termination of a transaction or the implementation of a business relationship.
- **"Freezing of funds"**- blocking of actual and/or legal movement of funds directly or indirectly owned or controlled by persons related to the spread of terrorism or weapons of mass destruction for an indefinite period, including blocking of the direct or indirect possession, use or disposal of such funds and prohibiting the establishment or execution of any Business relationship or Occasional Transactions.
- **"Client"**- a person who establishes a business relationship with the Company or is in such a relationship, as well as a person who offers the Company to perform or performs an Occasional Transaction.
- **"Beneficial owner"**- a natural person on whose behalf or for whose benefit the client actually acts and/or who actually controls the client or the person on whose behalf or for whose benefit the transaction is executed or the business relationship is established. A legal entity (except for trusts or other legal entities that do not have the status of a legal entity under foreign law) is considered to be a natural person if it:
 - a. directly or indirectly owns 20 percent or more of the voting shares (equities, shares) of the legal entity or directly or indirectly has 20 percent or more participation in the statutory capital of the legal entity,
 - b. carries out actual control over a legal entity by other means;
 - c. is an official person carrying out the general or current management of the activities of a legal entity in the event that there is no natural person meeting the requirements of subparagraphs "a" and "b".
- **"Authorized person"** - a person authorized to carry out a transaction or perform certain legal or actual actions in a business relationship on the Client's behalf and on the Client's instructions, including a person performing representation by a power of attorney or on another legal basis.
- **"Business Profile of a Client"**- a complete set of data about the nature, impact and significance of the Client's activity, the existing and expected dynamics, volumes and areas of the transaction or business relationship and Occasional Transactions, the presence,

identity and interrelationship of the Authorized Persons and Beneficial Owners, other facts related to the Client's activity and other information (images) about the circumstances of Client's activity.

- **"Client Simplified Due Diligence"** - the limited application of the Due Diligence process conducted by the Company, in which, during identification and identity verification, information provided by the Law, normative legal acts adopted by the Authorized Body and this Regulation is collected.
- **"Client Due Diligence"** - the process of collecting and analyzing information (including documents) on the identity and business activities of the Client using a Risk-Based approach to obtain a proper understanding of the Client, which includes the Law, the regulatory legal acts of the Authorized Body and this Regulation implementation of planned actions.
- **"Client Due Diligence Client"**- an extended application of the Client Due Diligence process conducted by the Company.
- **"Suspicious Transaction or Business Relationship"**- a transaction or business relationship, including an attempt to execute a transaction or establish a business relationship, in which it is suspected or there are reasonable grounds to suspect that the funds were obtained through criminal means or is related to terrorism, terrorist acts, terrorist organizations or with individual terrorists or terrorist financiers or has been used or intended to be used for terrorist purposes or by terrorist organizations or individual terrorists or terrorist financiers.
- **"Suspicious Transaction or Business Relationship Criterion"-situation** or an indication of the possibility of money laundering or terrorist financing defined by this Regulation and legal acts of the Authorized Body.
- **"Sanctions Lists"**- lists of the UN Security Council, US Office of Foreign Assets Control (OFAC), EU, UK HM Treasury (UK HMT). Within the framework of business agreements with partners, by the decision of the Company's shareholders' meeting, the list of Sanctions can be expanded to include lists of relevant countries and international bodies.
- **"Non-Cooperative Countries or Territories"**- a foreign country or territory that does not enforce or improperly enforce international requirements for the fight against ML/TF, in accordance with the lists issued by the Authorized Body.
- **"Center of Vital Interests"**- the location, where the family or economic interests of an individual are concentrated. The location of family or economic interests is the place, where the house (apartment) of the individual is located, where the individual and his/her family reside and his/her (family's) main personal and family assets are maintained, or where the main economic/professional activity is carried out.
- **"Politically Exposed Person/PEP"** - a person who has performed or performs significant functions of a state, political or public nature, as well as in an international organization (including a member of his family or a person closely related to him). Politically exposed persons are:
 - a. heads of state, government leaders, ministers, and deputy ministers;
 - b. members of the parliament;
 - c. members of supreme courts, constitutional courts or other high rank judiciary, whose

decisions

are not subject to appeal, except for special circumstances;

- d. the chairman of the central bank, his deputies and members of the board;
 - e. ambassadors, charges d'affaires and high rank officers of the armed forces;
 - f. political parties officials,
 - g. members of administration, management, or supervisory bodies of state-owned organizations;
 - h. heads of local self-government bodies;
 - i. international organization heads, deputy heads, board members or members of bodies performing other similar management or supervisory functions.
- **DB** - the "Depository Bank" software system used by the Company for the purpose of registration and accounting of transactions.
 - **"Unit Period"** -A period of one month.

1.5 Unless otherwise provided in this Regulation, the concepts used herein shall have the meaning provided by the Law.

1.6 This Regulation defines the functions and responsibilities of the Company's management bodies in the field of ML/TF and FPWMD prevention in the Company, including the responsible employees of the Internal Compliance Unit and other persons involved in the ML/TF process, the ML/TF risk criteria and the procedure for their determination, Client's identification, proper procedure for study, identification and management of the risks, the process of observation related to classifying the Transaction or Business relationship as suspicious, the procedure for collecting, recording and storing information and documents, the procedure for authorized persons and other employees in the field of ML/TF and FPWMD prevention, control over the implementation of the requirements of the Regulation and for the implementation of internal audit.

CHAPTER 2 FUNCTIONS OF THE COMPANY'S MANAGEMENT BODIES AND OTHER PERSONS IN THE FIELD OF ML/TF PREVENTION

2.1 The Company's Shareholders' Meeting:

2.1.1. approves Internal Audit reports and programs for the Internal Compliance Unit and ML/TF,

2.1.2. if necessary, instructs the responsible employees of the Internal Compliance Unit to carry out additional reviews of the transactions, established Business relations and employees' actions for compliance with the Law and the legal acts adopted on its basis,

2.1.3. approves measures aimed at eliminating deficiencies identified as a result of those reviews and monitors their implementation,

2.1.4. performs other functions defined by the Law and other legal acts adopted on its basis.

2.2 The Company's Executive Director

2.2.1. approves internal legal acts aimed at preventing ML/TF,

2.2.2. ensures full and effective implementation of the Law, Regulation and other legal acts adopted on the basis of the Law and exercises control over it,

2.2.3. appoints and dismisses responsible employees of the Internal Compliance Unit, ensures proper training of its employees in the field of ML/TF prevention,

2.2.4. ensures the implementation of measures aimed at eliminating deficiencies identified as a result of the studies conducted by the responsible employees of the Internal Compliance Unit, as well as the audit,

2.2.5. performs other functions defined by the Law and other legal acts adopted on its basis.

2.3 Mandatory measures in the field of ML/TF prevention also include conduct from responsible employees who establish direct contact with the Company's clients. They:

2.3.1. while establishing commercial, correspondent or other similar relations with the Client, as well as with foreign financial institutions, shall ensure the proper analysis of the latter and the collection, analysis and storage of the necessary documents and information in accordance with the requirements of this Regulation,

2.3.2. shall ensure the collection of necessary information on High-Risk Clients and providing it to the ICU for further analysis,

2.3.3. shall carry out current control and monitoring of clients and their accounts,

2.3.4. shall take measures to identify, recognize and prevent Suspicious Transactions by Clients or third parties, as well as in the cases defined by the Regulations or at the request of the ICU, immediately report information on Suspicious Transactions carried out by Clients or third parties to the ICU (Appendix 1),

2.3.5. during the implementation of the transaction, in the event of a match with the relevant lists checked by the Client or any of the parties and/or in the event of presence of a request to reject the Transaction, the relevant information shall be submitted to the ICU in accordance with Appendix 2 in order to obtain the appropriate permission for the rejection of the Transaction.

2.3.6. shall not inform other persons, as well as the person about whom information is provided to the ICU, about the fact of providing information.

CHAPTER 3 THE FUNCTIONS OF RESPONSIBLE EMPLOYEES OF THE INTERNAL COMPLIANCE UNIT

- 3.1** The functions of preventing money laundering and terrorist financing in the Company are placed on the responsible employees of the Internal Compliance Unit.
- 3.2** In carrying out the functions defined by the Regulation, the Law and the legal acts adopted on its basis, the ICU is independent and has the status of Senior Management, as well as the right of direct and immediate access to the information and documents available in the Company.
- 3.3** The ICU has the right to make a final decision to identify the Transaction or Business relationship as suspicious, to suspend, refuse or stop its implementation, to freeze the funds of persons related to terrorism, and inform the Executive Director and the Company's shareholders' board about the decision only after submitting the report to the competent authority on the suspicious transaction or business relationship, the decision on suspending business relations, refusing or terminating the implementation, freezing the financial funds or other funds of persons related to terrorism.
- 3.4** The employees of the company are obliged to provide any information that they believe will be necessary to perform the functions provided by the Regulation and to prevent money laundering and terrorist financing.
- 3.5** A responsible employee of the Internal Compliance Unit shall regularly, but not less than once every 6 months, examine the compliance of the Company's Transactions and established Business relation and the actions of the Company's relevant employees with the Regulation, the Law and other legal acts aimed at preventing money laundering and terrorist financing (Internal Report).
- 3.6** The internal study is carried out based on the decision of the responsible employee of the Internal Compliance Unit. A written decision on an internal study (Study Decision) is delivered to the Company's employees and the Company's CEO. The study decision outlines the purpose of the study, the terms of the study, and the list of documents and information to be provided by the Company's employees to the responsible employees of the Internal Compliance Unit and the terms of their provision.
- 3.7** The results of the study, the data on other mandatory measures provided by the Regulation and other issues raised by the Authorized Body are outlined in the report of the responsible employee of the Internal Compliance Unit which is submitted to the Executive Director of the Company within 10/ten/ working days after the end of the study period specified in the study decision. (Appendix 3).
- 3.8** The report referred to in Paragraph 3.7 includes:
- 3.8.1.** the number of Reportable Transactions, the number of Suspicious Transactions and Business Relationships and their brief description,
 - 3.8.2.** the number and brief description of the Transactions and Business relations on which analyzes were carried out, but were not qualified as suspicious,
 - 3.8.3.** the number and brief description of Transactions and Business relationships rejected or terminated by the Company,

3.8.4. the amount of frozen funds,

3.8.5. the number and brief description of suspended Transactions and Business relationships, information on the value of each suspended Transaction or Business relationship,

3.8.6. Cases of violation of the requirements of the Law, this Regulation and other normative legal acts adopted by the Authorized Body as a result of the actions of the company's employees.

3.9 As a result of the study of the current legislation and the performed analyses, the responsible employee of the Internal Compliance Unit, if necessary, submits the project that contains the draft of amendments and additions to the Company's Regulation developed by him, attached to the report specified in clause 3.7 of the Regulation. After the discussion of the project, it is submitted for the approval of the relevant management body of the Company.

3.10 Internal Compliance Unit:

3.10.1. summarizes and reviews information received from the Authority on "Terrorist Suspects" and related persons, persons on the Authority's, UN Security Council's, OFAC, EU and UK lists, also using the World Check database and ensures the access to the responsible employees who establish direct contact with the Company's clients. At the same time, the procedure for checking the compliance of the Clients' list of Sanctions is defined by the Company's "Sanctions Compliance" policy.

3.10.2. on a daily basis, the DB program checks the transactions subject to additional analysis carried out by the responsible employees establishing direct contact with the Company's clients,

3.10.3. verifies all international transactions, regardless of the size of the amount and the client's business characteristics, performing additional analysis,

3.10.4 carries out the collection, summarization, and storage of information on mandatory reporting and Suspicious transactions submitted to the ICU by the responsible employees who establish direct contact with the Company's clients,

3.10.5 In order to effectively implement the functions related to the prevention of ML/TF, provides support and advice to other competent employees in the field of ML/TF prevention, as well as provides clarifications to the employees of the Company regarding issues arising during the implementation of measures aimed at combating ML/TF,

3.10.6 ensures the provision of reports and other information on the Transactions subject to mandatory reports to the Authorized Body on behalf of the Company as well as ensures the Company's communication with the Authorized Body,

3.10.7 In order to identify Suspicious Business Relations or Transactions, conducts, analyzes, studies and saves the results (Appendix 4), including the data and suspicions about the Suspicious Transaction or Business Relationship, in connection with which the Suspicious Transaction or Business Relationship Report was submitted to the Authorized Body,

3.10.8 ensures risk assessment of the Company's Clients and Transactions (Business Relationships) classification according to the degree of Risk, carries out regular review and current monitoring of compliance with the given risk group, observes the

current monitoring of the Transaction/Business Relationship and periodically reviews the process of information adjustment and updating,

- 3.10.9** makes a decision to qualify the Business relationship or the Transaction as suspicious, to suspend it, to refuse its implementation, to freeze the financial funds related to the spread of terrorism or weapons of mass destruction, discusses the matter as necessary with other employees who provide internal feedback and serve the Clients, and in case of disagreement, makes a final decision,
- 3.10.10** carries out the functions of monitoring, collecting information, recording, storing and regularly updating information systems operating in the Company in the field of ML/TF prevention,
- 3.10.11** organizes internal training and training in the field of money laundering and terrorist financing, monitors the progress and results of training programs,
- 3.10.12** develops internal legal acts for combating money laundering and terrorist financing, submits them for approval to the relevant body, monitors their effectiveness, makes proposals for increasing effectiveness,
- 3.10.13** performs other functions defined by the Law and other legal acts adopted on its basis,
- 3.10.14** performs other functions assigned by the management bodies of the Company to the extent that it does not limit the independence of the Internal Compliance Unit.

CHAPTER 4. ML/TF RISK CRITERIA AND THE RISK IDENTIFICATION PROCEDURE

- 4.1** When reviewing a client or a transaction (business relationship), the Company classifies them according to high, low and medium (standard) Risk criteria.
- 4.2** The risk is assessed according to the criterion characterizing the risk, and in the presence of more than one criterion, by their combination.
- 4.3** Risk is assessed as low when only low risk criteria are present. Low risk criteria indicate a low probability of ML/TF. Low risk criteria are presented in the following:
- 4.3.1** effectively supervised financial institutions from the point of view of combating ML/TF,
 - 4.3.2** state bodies, local self-government bodies, state non-commercial organizations, state administrative institutions, with the exception of those bodies or organizations that are located in such countries (territories) where the international requirements for combating ML/TF are not applied or not properly applied.
- 4.4** Risk is rated High when at least one High Risk criterion is present. High Risk criteria are presented in the following persons, events or objects:
- 4.4.1** a potential or existing Client or Beneficial Owner who is a person with political influence or has a member of his family with political influence or a person connected to him,
 - 4.4.2** legal entities involved in a transaction or business relationship (including financial institutions) located in countries (territories) where (according to the lists established by the Central Bank of the Republic of Armenia and relevant international organizations) money laundering and terrorist financing are not applied or are improperly applied,
 - 4.4.3** complex or unusually large amount of Transactions, Transactions with unusual conditions or Business relations, the economic or other legal purposes of which are not obvious,
 - 4.4.4** involvement in a transaction or business relationship of a legal entity or organization whose field of activity is individual management of assets,
 - 4.4.5** charitable or non-profit organizations,
 - 4.4.6** involvement of a company that has registered or bearer shares in a transaction or business relationship,
 - 4.4.7** the cases where there is a Transaction or Business relationship characterized by large-scale use of cash,
 - 4.4.8** involvement in a Transaction or Business Relationship of a company that has an unusual or unnecessarily complex structure of owners;
 - 4.4.9** the cases when there are doubts about the previously acquired data for identification, including the existence of the Beneficiaries and the authenticity of the data about them,
 - 4.4.10** a transaction is requested by Clients whose accounts have frequent and unexplained movements of funds to various financial institutions,
 - 4.4.11** clients are involved or interested in the transaction, and the structure or nature of

the Transactions and/or Business relations carried out by them makes it difficult to identify the Beneficiary;

4.4.12 the transaction is performed between a natural person affiliated with a legal entity and another legal entity for the purpose of fulfilling contractual obligations between these legal entities,

4.4.13 Transaction and/or Business relationship without face-to-face contact,

4.4.14 the cases when it becomes known that the establishment of the Business relationship with the Client or the execution of the Transaction was rejected by another financial institution,

4.4.15 Other criteria.

4.5 The ML/TF Risk of a Transaction (Business Relationship) is assessed as Medium when the High or Low Risk criteria are not met.

4.6 The risk is evaluated as high in the event of presence of at least one criterion of high risk.

4.7 In case of simultaneous presence of several criteria for different risks, the risk is evaluated in accordance with the most risky of the existing criteria.

4.8 It is prohibited to enter into a Transaction and/or establish a business relationship with persons engaged in the following types of activities characterized by the highest risk in the field of money laundering and terrorist financing prevention:

4.8.1 With persons, military agencies and other organizations engaged in the production, purchase and sale of weapon(s) and/or their use for offensive purposes.

4.8.2 Organizations engaged in the manufacturing, preparation, processing, sale, and distribution of any form of narcotics, psychotropic (psychoactive) substances, their preparations, or analogous substances (analog) or derivatives, as well as organizations associated with enterprises that provide support for these activities.

4.8.3 With organizations operating in the field of atomic energy production.

4.8.4 With organizations offering services, that are subject to the restrictions outlined in the Law of the Republic of Armenia on "Trade and Services".

4.8.5 With banks that do not have a physical presence in the country of registration and licensing, and not affiliated with any regulated financial group under effective consolidated supervision; "Physical presence" refers to the existence of management personnel within a respective country. The presence of a local agent or non-management personnel does not qualify as physical presence.

4.8.6 With unregulated charitable organizations that are not subject to the control of any state and/or local government authority.

4.8.7 With any person or legal entities providing virtual assets (crypto-assets) services which perform one or more of the following actions or operations for or on behalf of another person or legal entity:

4.8.7.1 exchanging virtual assets for fiat currencies;

4.8.7.2 exchanging between one or more forms of virtual assets;

4.8.7.3 transfer of virtual assets;

4.8.7.4 preserving and/or managing virtual assets or tools that grant control over virtual assets;

4.8.7.5 provision of financial services related to the issuance and/or sale of virtual assets.

- 4.9** The company conducts a supplementary examination of the client for businesses operating in the following sectors, and it proceeds with finalizing transactions and/or establishing business relations under certain restrictions:
- 4.9.1** the sector of lotteries, games of chance, internet-based games of chance, and casinos. This encompasses both entities with physical establishments and online/remote gambling businesses. The Company does not enter into a transaction and/or establish a business relationship with persons operating in the given field who are not properly licensed and/or do not have the minimum customer due diligence procedures in the field of money laundering and terrorist financing prevention.
 - 4.9.2** Money or other financial instruments transfer services (MVTs) sector, which refers to those financial services (excluding banks) that encompass the acceptance of cash, checks, and other payment instruments, disbursing the equivalent amount to the beneficiary, either in cash or through other methods such as messaging, transfers, or the clearing network affiliated with the financial service provider. The Company does not enter into a transaction and/or establish a business relationship with persons operating in the given field who are not properly licensed and/or do not have the minimum customer due diligence procedures in the field of money laundering and terrorist financing prevention.
 - 4.9.3** Payment service providers, functioning as third-party entities in the payment processing process, enable businesses to accept payments through diverse online payment methods. The Company does not enter into a transaction and/or establish a business relationship with persons operating in the given field who are not properly licensed and/or do not have the minimum customer due diligence procedures in the field of money laundering and terrorist financing prevention.
- 4.10** In the event that any new criteria of Risk arise during the Business relationship with the Client, the Internal Compliance Unit of the Company reviews the assessment of the given Risk and, in the event of a change in Risk, implements Due Diligence measures of the Client provided for by the Law and this Regulation for the newly determined Risk.
- 4.11** From the day of receiving information about the Company's clients, the responsible employee, who makes direct contact with the Company's clients, classifies the latter according to Risk: High, Low or Medium (standard) criteria. In the event that, in the opinion of the Company's employee, the Client should be qualified as a Client of High Risk criteria, he immediately informs the responsible employee of the Internal Compliance Unit about it, and upon receiving a request from the responsible employee of the Internal Compliance Unit, he provides him with the information that was the basis for the Client to be considered as a High Risk Client.
- 4.12** From the moment of receiving information (application or instruction) regarding the Transaction or Business relationship to be carried out for the Company's Clients, the responsible employee, who establishes direct contact with the Company's Clients, classifies it according to Risk: High, Low, or Medium (standard) criteria. In the event that, in the opinion of the Company's employee, the Transaction (Business relationship) should be qualified as a Transaction of High Risk he immediately informs the responsible employee of the Internal Compliance Unit about it, and upon receiving a request from the responsible employee of the Internal Compliance Unit, provides him with the information, which were the basis for considering the Client or a Transaction (Business Relationship) of High Risk criteria.
- 4.13** The company reviews its potential and existing risks of money laundering and terrorist financing once a year.

CHAPTER 5. CUSTOMER IDENTIFICATION, CORRESPONDENCE AND DUE DILIGENCE, RISK IDENTIFICATION AND MANAGEMENT

5.1 The Company establishes a Business relationship with the Client (Authorized Person) or concludes an Occasional Transaction with the Client after receiving the information and documents provided by this Regulation and the Law for the identification of the Client and verifying the Client's identity. The company does not establish a Business relationship or make an occasional transaction without first verifying the Client's identity.

5.2 The employee who establishes direct contact with the Client shall identify the Client and verify their identity based on legible and valid documents and other information provided by the competent state authorities. When identifying and verifying the identity of the Client (Authorized Person):

5.2.1 The information required for natural persons and individual entrepreneurs based on an identification document or another valid official document exceptionally with a photo shall at least include: the person's first and last names, citizenship, registration address (if any), date and place of birth, details of the identity document including series, number and date of issuance, and for individual entrepreneurs, also the registration number and taxpayer identification number, as well as other information required by the legislation and other internal legal acts of the Company. The employee who establishes direct contact with the Client shall also find out the Client's place of residence.

5.2.2 The information required for legal entities, obtained on the basis of the state registration document or other official documents should at least include the name, location, identification number of the legal entity (state registration, registration number, etc.), the CEO's first and last name, and, if available, the taxpayer's name, the registration number. The information shall also include the charter, if available, its amendments and appendices. In the case when the legal entity's activity is subject to licensing, the corresponding license/permit shall be produced, as well as other information and documents required by the legislation and other internal legal acts of the Company if necessary.

5.2.3 The information required for a state body or local government body shall at least include the full official name of the state body or local government body and the country.

5.3 In case of establishing a Business relationship with the Company, the Client shall fill in the "Identification and verification Questionnaire" in accordance with the relevant annexes of the Company's FATCA requirements compliance policy implementation and assurance policy.

5.4 The electronic version of the completed questionnaire and other documents necessary for identification in accordance with 5.3 of this Regulation shall be recorded in the Client's section of the DB software system by the employee who establishes direct contact with the Client.

5.5 Information obtained during the Client's identification is verified by an employee who contacts the Client directly and, if necessary, by the ICU and other subdivisions and employees, in accordance with the Regulation.

5.6 In the event of a positive response received by ICU from an e-mail sent by the employee establishing direct contact with the Client and on the basis of the information required for

identification, the identity of the Client is verified during the establishment of a business relationship or after a reasonable period, which does not exceed seven days, if the risk is effectively managed, and it is necessary in order not to disrupt normal Business relations with the Client.

5.7 Due diligence of the Client (Authorized Person) is mandatory in the following cases:

5.7.1 a Business relationship with the Client (Authorized person) is established,

5.7.2 an occasional transaction is performed

5.7.3 suspicions arise with regard to the veracity or adequacy of previously obtained Client's (Authorized Person's) identification data,

5.7.4 there are suspicions about ML/FT

5.8 In the cases provided for in 5.7 of this Regulation, the responsible employee of the Internal Compliance Unit conducts a Due Diligence of the Client, taking measures appropriate to the ML/TF Risk. During the Due Diligence of the Client, the responsible employee of the Internal Compliance Unit shall conduct an observation of the existing or potential Client and the Transaction with the latter in order to ensure the existing information on the Client, his Business profile and risk, and, if necessary, the authenticity of their source of income.

5.9 The Client's Due Diligence process includes identifying and verifying the Client (Authorized Person or Beneficial Owner), determining the purpose and intended nature of the Business Relationship, and conducting ongoing due diligence throughout the Business Relationship (including the moment the Client enters into a Business Relationship).

5.10 In the event that the Client has been classified as a Low Risk Client, the responsible employee of the Company's Internal Compliance Unit conducts a Simplified Study of the Client. Simplified Client's Study includes the collection and study of the following information about the Client:

5.10.1 in the case of a natural person,

5.10.1.1 the name, the last name,

5.10.1.2 identity document information,

5.10.1.3 Information on the authorized person provided for 1n clauses 5.10.1.1-5.10.1.2 (if available).

5.10.2 In the case of a legal entity

5.10.2.1 the name,

5.10.2.2 the certificate of legal registration,

5.10.2.3 Information identifying the person authorized to manage the account.

5.11 In case, when establishing Business relations with the Client, the latter is classified as a Client of the Low risk criteria, the responsible employee of the Internal Compliance Unit carries out reduced measures of due diligence of the Business relationship.

5.12 Within the framework of Due diligence in the case of low risk, the responsible employee of the Internal Compliance Unit shall undertake the following activities:

5.12.1 to verify the authenticity and reliability of the information and documents required from the Client in relation to the Transaction or Business relationship, based on the information provided by the Client,

5.12.2 to review the sources, movements and volumes of the Client's funds circulating in different Transactions during a given period only when they exceed a reasonable amount limit in terms of the Client's Business Profile,

5.12.3 to identify connections between Clients, Transactions and Business Relationship

only when connections to Medium or High Risk Clients, Transactions or Business Relationship are evident.

5.13 In the case of Medium Risk, the responsible employee of the Company's Internal Compliance Unit conducts Client's Due Diligence and undertakes regular ongoing Due Diligence activities of the Business Relationship.

5.14 In the case of Medium Risk, the responsible employee of the Internal Compliance Unit undertakes the following measures in order to monitor Client's Transactions within the framework of the current Due Diligence:

5.14.1 verifies the reliability and completeness of the Client's information and documents regarding a Transaction or Business Relationship, using, if necessary, information with limited availability and publicly available sources, making inquiries from competent authorities and other accountable informants as well as from foreign partners,

5.14.2 at least once a year analyzes the sources, movement and volumes of the Client's funds circulating in different Transactions during the given period,

5.14.3 at least once a year identifies the existence of links between Clients, Transactions and Business Relationships

5.14.4 verifies the compatibility of Transactions or Business Relationship with the Client's Business Profile.

5.14.5 identifies the source of the Client's income and assets.

5.15 The responsible employee of the Company's Internal Compliance Unit conducts an Additional Due Diligence of the Client in cases where the Client and/or the Transaction carried out by him were classified as High Risk, as well as in accordance with Part 1 Clause 6 Article 10 of the Law on the implementation of an additional Due Diligence of the Client in cases where there is an order to do so. In case of conducting an additional Due Diligence in addition to the actions defined by the Due Diligence of the Client, the responsible employee of the Internal Compliance Unit shall also:

5.15.1 carry out verification of the presence of the real beneficiary based on the statement filled out by the Client in the appropriate form defined by the Regulation in accordance with Appendix 1 of "Customer Classification and Information Exchange Regulation",

5.15.2 receive the approval of the Company's Senior Management before establishing a Business relationship with the Client or continuing it, as well as in cases where it was later determined that the Client, the Beneficiary Owner, the Transaction or the Business relationship is characterized by the High Risk criterion,

5.15.3 take necessary measures to find out the source of the Client's income and assets,

5.15.4 examine in detail the prerequisites and purpose of the Transaction or Business Relationship,

5.15.5 in the case of a person with political influence, carries out additional current Due Diligence.

5.16 In the framework of the current Due Diligence of the business relationship, for the purpose of monitoring the Client's Transactions, the responsible employee of the Internal Compliance Unit shall undertake the following advanced measures in case of high risk:

5.16.1 when verifying the veracity and reliability of the information and documents obtained from the Client in connection with the transaction or business relationship, the responsible employee shall request the necessary information (including additional documents), use information with limited availability and publicly available sources, makes

inquiries from the largest possible number of competent authorities and other accountable persons, as well as from foreign partners,

5.16.2 when comparing the sources, movement and volumes of the Client's funds circulating in different Transactions, the responsible employee shall choose the longest possible period or several comparable periods,

5.16.3 at least once every 6 months (in the case of persons with political influence: once every 3 months) when determining the existence of connections between Clients, Transactions and Business relations, the responsible employee shall perform a multi-level analysis of them in order to identify possible indirect connections,

5.16.4 when checking the comparability of any Transaction or Business relationship with the Client's Business Profile, the responsible employee shall identify the information and documents fully justifying the actions performed by Client.

5.17 When conducting an Additional Due Diligence of the Client, the responsible employee of the Internal Compliance Unit shall at least require:

5.17.1 For a natural person who is a citizen of the Republic of Armenia:

5.17.1.1 An identification document,

5.17.1.2 A document containing registration plate of public services or a reference to not having it.

5.17.1.3 Statement on the source of the Client's (Beneficiary's) assets and funds, which requires additional study and analysis.
As well as

5.17.1.4 additional documents, contracts, payment receipts, or other supporting documents.

5.17.2 For a foreign natural person,

5.17.2.1 Passport of a foreign state or an internationally recognized document confirming the person (identity) or special passport or residence card,

5.17.2.2 Identification card (if present),

5.17.2.3 Statement on the source of the Client's (Beneficiary's) assets and funds, which is necessary for additional study and analysis,

5.17.2.4 Additional documents, contracts, payment receipts, or other supporting documents.

5.17.3 For a legal entity registered in the Republic of Armenia:

5.17.3.1 A registration certificate,

5.17.3.2 A document containing the tax payer's number (if the state registration certificate does not contain such information),

5.17.3.3 A list of persons authorized to manage and/or sign bank accounts, the head of the executive body of the company, identification documents and samples of signatures, approved by the relevant authority of the company,

5.17.3.4 Additional documents, contracts, payment receipts, or other supporting documents.

5.17.4 For a foreign legal entity,

5.17.4.1 Registration certificate and (or) other founding document,

5.17.4.2 Extract from the commercial register of the country of registration or other equivalent document confirming the legal status of a foreign legal entity, the

expiration date of which should not exceed 12 months,

5.17.4.3 A list containing the head of the executive body of the company, the persons authorized to manage and/or sign the accounts, identification documents and samples of signatures, approved by the relevant authority of the company,

5.17.4.4 Statements on the sources of assets and funds of significant participants (shareholders) and beneficiaries of the company, which are necessary for additional study and analysis,

5.17.4.5 additional documents, contracts, payment receipts, or other supporting documents.

5.18 When a Client is found to meet the High Risk criteria during identification, the Client's accounts are activated only after additional Due Diligence has been conducted with the permission of ICU. In particular ICU shall carry out the following measures:

5.18.1 conduct a more complete and in-depth verification of the veracity of the documents (information) required when establishing business relations with the Client, request other supporting documents (information),

5.18.2 request information on the source of the Client's assets and funds;

5.18.3 examine the Client's information and Business Relationship and Transaction information in databases

5.18.4 make requests to other reporting entities, including foreign partners to verify information about the Client, Business relations with him and Occasional transactions, 5.18.

5.18.5 carry out in-depth monitoring of Transactions,

5.18.6 take other measures to get a real and complete picture of the Customer, his Transactions and his Business relationships.

5.19 Business relations without face-to-face contact are regulated by the Company's internal procedure "On Establishment of Business Relations Without Face-to-Face Contact". When establishing Business relations without face-to-face contact, the Company, within the framework of due diligence of the Client, requires that the first payment be made to an account opened in the name of the Client at a financial institution that

5.19.1 is eligible and may promptly provide, upon request, information obtained as a result of Customer Due Diligence, including copies of documents.

5.19.2 In terms of combating ML/TF, is subject to proper regulation and control. It also has effective procedures for due diligence of the Client and storage of information defined by the Law and legal acts adopted by the Authorized Body

5.19.3 is not in a country or territory where the international requirements for money laundering and financing of terrorism are not applicable or inappropriate.

5.20 Before establishing a Business relationship or concluding an Occasional Transaction, the Company identifies the Client's business Profile, as well as specifies the type and intended nature of the Transaction or Business relationship.

5.21 The Company shall take measures to determine whether the Customer, a member of his family or a person related to him is a Politically Influenced Person by checking the Customer's data from international lists, especially the UN Security Council Resolutions, OFAC, EU, UK, internal lists provided by the Authorized Body and World Check database. For this purpose the Company shall also conduct the necessary research on the Internet (Google, Facebook, Twitter, LinkedIn, etc.) in Armenian, Russian, English or other languages.

5.22 Before establishing a Business relationship or concluding an Occasional Transaction, the Company shall detect the presence of the Beneficial Owner and, if there is one, the Company shall identify him and verify his identity. In the case of legal entity clients, the Company obtains full information on the powers of the participants and management bodies of the legal entity (except for reporting issuers provided for by the securities regulation legislation) in order to identify the Beneficial Owner. If the Company detects the presence of the Beneficial Owner, "Statement on the existence (absence) of the Beneficial Owner" shall be filled out in accordance with Appendix 5. "Declaration on the existence (absence) of the Beneficial Owner" is also completed when the Beneficial Owner appears or changes during the Business relationship.

5.23 In the event when the Client has been classified as a Low Risk Client, the Beneficial Owner identification and identity verification requirements for Low Risk Clients under this Regulation shall apply.

5.24 The Company identifies the center of vital interests of the Client who is a foreign legal entity or a foreign natural person or a Client who does not have the status of a legal entity under foreign law. When identifying the center of vital interests, a "Declaration on the Center of Vital Interests" is completed in accordance with Appendix 1 of "Customer Classification and Information Exchange Regulation". "Declaration on Center of Vital Interests" is also completed if the Center of Vital Interests presented in the original declaration changes during the Business Relationship.

5.25 Under the conditions established by the Law, the information obtained as a result of the due diligence of the Client by another financial institution or non-financial institution or other authorized bodies may serve be used for the Company when conducting due diligence of the Client.

5.26 The Company can have Business relations with the Client, conclude Transactions, including Occasional Transactions, only after he has opened an account with the Company. An account can also be opened online (on the Company's website or via the provided link). In the cases where the Client wishes to open an account without face-to-face contact with the Company's employees by filling out an online application, the Client will download the electronic versions of the following documents when filling out the account opening application on the website, namely:

5.26.1 For natural persons:

5.26.1.1 identity document or other official document (passport, identification card) exclusively with a photo,

5.26.1.2 a document confirming the person's residential address, provided by a third party, in particular, a bank reference or bank account statement regarding the Client, a receipt for payment of utility services, where the first and last name and residential address are clearly visible, or another document that meets the requirements of this clause. The documents defined in this clause must be provided no earlier than within 3 months prior to its submission to the Company. The requirement from this clause does not apply in cases where the Client's identity document contains information about his place of residence.

5.26.1.3 Information about the person's business profile, the purpose and intended nature of the business relationship.

5.26.1.4 For a natural person who is not a resident of the Republic of Armenia, information about the center of vital interests shall include:

5.26.1.5 a statement on the beneficial owner, including the documents and

information mentioned in sub-clauses 5.26.1.1-5.26.1.4.

5.26.1.6 information on whether the person is acting on his own behalf or on behalf of someone else. In case of acting on behalf of another person, the Client shall produce a document confirming the authority and the document and information about the authorizing person specified in sub-clauses 5.26.1.1-5.26.1.4.

5.26.2 For legal entities:

5.26.2.1 the state registration document or other official documents on registration, which shall include the name of the legal entity, location, personalization number (state registration, registration number, etc.), the name of the head of the executive body and, if available, the taxpayer's registration number,

5.26.2.2 the company's charter or other document on the powers of management bodies,

5.26.2.3 the information on the beneficial owner (except for reporting issuers provided for by the securities market regulation legislation), as well as other documents on the beneficial owner mentioned in sub-clauses 5.26.1.1-5.26.1.4,

5.26.2.4 the documents confirming the authority of the person acting on behalf of the company, as well as the documents and information provided for in sub-clauses 5.26.1.1-5.26.1.4 regarding the person acting on behalf of the company,

5.26.2.5 the information on the business profile of the legal entity, the purpose and intended nature of the business relationship,

5.26.2.6 the actual business address,

5.26.2.7 Information about the center of vital interests for a legal entity that is not a resident of RA or an organization that does not have the status of a legal entity.

5.27 The Company conducts ongoing due diligence throughout the business relationship. Ongoing due diligence includes monitoring transactions of the Client (Authorized Person) in order to ensure the reliability of available information about the Client, its business profile and risk, the comparability of the Client's activities with other information, and, if necessary, the veracity of the source of the Client's income and assets. ICU conducts monitoring throughout the business relationship (including the moment of establishing a business relationship with the Client). The measures are taken at the following intervals:

5.27.1 once every three months, in the case of persons with political influence,

5.27.2 once every six months, in the case of clients at high risk,

5.27.3 once a year, in the case of clients at a medium (standard) risk.

5.28 The information collected as part of Client's due diligence (except for information obtained as a result of Client's identification and identity verification, which is updated no less than once a year) is updated at the following intervals:

5.28.1 once every three months, in the case of persons with political influence,

5.28.2 once every six months, in the case of clients at high risk,

5.28.3 once a year, in the case of clients at medium (standard) risk,

5.28.4 once every two years in the case of clients at low risk.

5.29 When determining the customer's business profile, the ICU must ensure that it has obtained sufficient information to determine the fact that the Customer is a Politically Influential

Person.

5.30 Reliable employees who establish direct contact with the Client, when making a Transaction or establishing a Business relationship, must act as defined in Appendix 7 of this Regulation.

CHAPTER 6. THE REVIEW PROCESS (ANALYSIS) RELATED TO THE SUSPICIOUS TRANSACTIONS, INFORMATION, OR BUSINESS RELATIONSHIP

6.1 The Company provides the authorized body with reports on the following transactions:

6.1.1 non-cash transactions, the amount of which is equal to or exceeds 20 million AMO,

6.1.2 cash transactions, the amount of which is equal to or exceeds 5 million AMO,

6.1.3 Suspicious transactions or business relationships, regardless of the amount of the transaction provided for in sub-clauses 6.1.1 and 6.1.2.

6.2 It is prohibited to inform the person on whom a report or other information is provided to the Authorized Body or other persons about the fact of providing the report or other information.

6.3 The procedure for drawing up the reports mentioned in clause 6.1 of this Regulation and providing them to the Authorized Body is defined by the Law, normative legal acts adopted on its basis, this Regulation and other internal legal acts adopted on its basis.

6.4 In order to ensure the preparation of the reports mentioned in Clause 6.1 of this Regulation, the Company's employees, on the day of performing the Transaction or discovering the basis of the Suspicious Transaction (Business Relationship), provide the responsible employee of the Internal Compliance Unit with the necessary documents and information to prepare the report and submit it to the Authorized Body.

6.5 The process of assessing the transaction or business relationship as suspicious is carried out by the ICU in accordance with the procedure established by the Regulation, the Law and other legal acts adopted on its basis.

6.6 The process of assessing a transaction or business relationship as suspicious begins upon receipt of internal or external signals, as well as upon the initiative of the responsible employee of the Internal Compliance Unit in all cases when:

6.6.1 there is a possible overlap between the data of the Client or the other party to the transaction and the identification data of persons related to terrorism or other persons specified in the instructions of the Authorized Body,

6.6.2 the observed situation fully or partially corresponds to the cases defined by the guideline "On the criteria of high risk and suspiciousness of money laundering and financing of terrorism" which establishes the criteria and types of a suspicious Transaction or Business relationship, approved by the decision of the President of the Central Bank of RA NQ. 1/711-A from October 11, 2016,

6.6.3 the terms of the Transaction (Business Relationship) do not correspond to the Client's business profile or to the terms of such Transactions (Business Relationships) usually concluded in the given field of business activity, or to the customs of business circulation,

6.6.4 it becomes obvious to the Company that the volume of the proposed or concluded transactions does not exceed the limit necessary for the provision of the report and the

identification of the Client provided for in this Regulation only because the Client wants to avoid the provision of the report on that transaction or identification procedure conducted by the Company,

- 6.6.5** the logic, movement (dynamics) or other circumstances of the execution of the concluded or proposed Transaction or Business relationship give reason to believe that it can be carried out for the purpose of ML/TF,
- 6.6.6** it becomes clear to the Company that the proposed or concluded Transaction (Business Relationship) does not pursue an obvious economic or legal purpose,
- 6.6.7** a natural person, who is affiliated with any legal entity, transfers (provides) money (securities) to another legal entity on his behalf, which is obviously carried out for the purpose of fulfilling contractual obligations between these legal entities or for carrying out business activities between these legal entities in another way,
- 6.6.8** there are other circumstances indicating the suspicious Transaction or Business relationship.

6.7 Internal signals are the signals (information) transferred to the ICU by the reliable employees who establish direct contact with customers, the management bodies of the Company, the Internal Audit, as well as other competent employees in the field of ML/TF prevention.

6.8 External signals are the signals received from the Authorized Body, competent authorities, other reporting persons, foreign partners, as well as from sources with limited access to information and publicly available sources.

6.9 In the case defined by sub-clause 6.6.1 of the Regulation, when there is a possible match

with the identification data of other persons specified in the instructions of the Authorized Body, the responsible employee of the Internal Compliance Unit shall carry out appropriate comparisons and a positive match within the terms specified in the order, as well as in the case when it is not possible to ensure the absence of a positive match and perform the actions defined by the instructions.

6.10 In the case defined by sub-clause 6.6.1 of the Regulation, when there is a possible match with the identification data of persons related to terrorism, the responsible employee of the Internal Compliance Unit immediately shall carry out appropriate comparisons and a positive match, as well as in the case when it is not possible to ensure the absence of a positive match, submit a report to the Authorized Body on suspicious transaction and make a decision on Freezing the Customer's funds.

6.11 In the cases specified in Article 6.6, sub-clauses 6.6.2-6.6.8 of the Regulation, the ICU performs a comprehensive analysis within a reasonable time using the information collected and additionally acquired within the framework of the due diligence of the Client. If necessary, it makes clarifications with the financial observation center of the Central Bank of RA and if the Transaction or Business relationship is believed to be suspicious, submits a report on the suspicious Transaction or Business relationship to the Authorized Body in accordance with the procedure established by the Law, and also takes other measures prescribed by the Law.

6.12 In case where the employee of the Company detects one or more Suspicious Transactions or has doubts about it, he submits a notification (electronically or in paper form) to the responsible employee of the Company's Internal Compliance Unit, which indicates the basis for considering the Transaction (Business Relationship) as suspicious, and also attaches all the documents that will be necessary to carry out an appropriate investigation.

- 6.13** The notification defined by sub-clause 6.1.2 of the Regulation is made by the employee in accordance with Appendix 1.
- 6.14** The responsible employee of the Internal Compliance Unit shall perform an additional analysis of the submitted information and prepare a conclusion on the same day of receiving the information from the Company's employee.
- 6.15** ICU compares the Client's data with the World-Check database, in particular with the database of the PEPs (or other database used by the Company), as well as with the information available on other publicly accessible websites through the Internet, checking the veracity of the information.
- 6.16** The ICU, combining the information provided by the employee in direct contact with the Clients and received from other sources, as well as collected as a result of its own observations, makes a final decision to assess the Transaction or Business relationship as suspicious, to suspend, reject or stop its implementation, to freeze the funds of persons related to terrorism.
- 6.17** The responsible employee of the internal monitoring body uses the information collected and additionally obtained within the framework of the due diligence of the Client when performing analyses, and if necessary, makes clarifications with the Financial Monitoring Center of the Authorized Body. If as a result of the analysis, the Internal Monitoring Officer finds out that all the criteria for a Suspicious Transaction (Business Relationship) provided by this Regulation and the Law are not present or the grounds for considering the Transaction (Business Relationship) suspicious are insufficient, the responsible employee of the Internal Compliance Unit informs the Company's employee about this decision. The notification can be submitted by writing "Allow the transaction" on the form provided by the Company employee to the responsible employee of the Internal Compliance Unit or by sending a message containing the notification "Allow the Transaction" to the Company employee by e-mail, attaching the form provided by the Company employee to the responsible employee of the Internal Compliance Unit.
- 6.18** In the event where there are grounds for Freezing the Client's funds, the responsible employee of the Internal Compliance Unit submits the information to the Company's employee with the record "Freeze funds". From the moment of accepting the decision on Freezing, the ICU immediately defines the Transaction or Business relationship as suspicious and submits a report on the Suspicious Transaction or Business relationship to the Authorized Body.
- 6.19** If, on the basis of internal and external signals, or as a result of the analysis carried out on its own initiative, the ICU does not assess the Transaction or Business relationship as suspicious, and does not provide a report on the suspicious Transaction or Business relationship to the Authorized Body, then the justifications for closing the Transaction or Business relationship as suspicious, the conclusions of the responsible employee of the ICU, analysis process and results made by him are documented (according to Appendix 4) and stored for 5 years.

CHAPTER 7. SUSPENSION OF A SUSPICIOUS TRANSACTION OR BUSINESS RELATIONSHIP, REJECTION OR TERMINATION OF IMPLEMENTATION OF A TRANSACTION OR BUSINESS RELATIONSHIP AND FREEZING THE FUNDS OF PERSONS LINKED TO TERRORISM

7.1 In case of suspicion of money laundering or financing of terrorism, the Company has the right to suspend the Transaction or Business relationship for up to 5 days. And if the Company receives an instruction specified in Part 1, Clause 6, Article 10 of the Law, it shall immediately make a report about the suspicious Transaction or Business relationship to the Authorized Body.

7.2 The Company shall immediately execute the decision of the Authorized Body to suspend the Transaction or Business Relationship.

7.3 The decision of the Company or the Authorized Body to suspend the Transaction or Business Relationship before the end of the suspension period can only be cancelled by the Authorized Body on its own initiative or through the mediation of the Company, if it turns out that the suspicion of ML/TF is unfounded.

7.4 In the event where it is not possible to carry out the due diligence of the Client, or there is an instruction to refuse the implementation of the Transaction or Business Relationship by the Authorized Body, the Company must reject the implementation of the Transaction or Business Relationship and qualify it as suspicious.

7.5 In the event specified in Article 5.6 of the Regulation, if after establishing a Business relationship, it is not possible to carry out the due diligence of the Client or there is an order from the Authorized Body to terminate the Transaction or Business relationship, the Company must terminate the Transaction or Business relationship and qualify it as suspicious.

7.6 Funds directly or indirectly owned or controlled by persons linked to terrorism, included in the lists published in the resolutions of the United Nations Security Council, as well as by those included in the lists published by the Authorized Body, shall be frozen by the Company immediately and without prior notification.

7.7 The freeze is only lifted by the Authorized Body if funds are frozen by error, frozen by a law enforcement agency, or when it is discovered that the person whose funds have been frozen has been removed from the list of persons linked to terrorism.

7.8 If the Company freezes the funds of persons related to terrorism, the Transaction or Business relationship is immediately classified as suspicious and the Company shall provide the Authorized Body with a report on the suspicious Transaction or Business relationship.

7.9 The subject of freezing cannot be the funds that belong to a bona fide third party, that is, a person who, when providing the funds to another person, did not know or could not have known that it will be used or intended to be used for criminal purposes, including terrorism or terrorist financing, as well as to the person who, when acquiring the funds, did not know or could not have known that it was obtained by criminal means.

CHAPTER 8. PROCEDURE FOR COLLECTION, ACCOUNTING AND STORAGE OF INFORMATION AND DOCUMENTS

8.1 When establishing a Business relationship with the Client (Authorized Person), the Company may require from him all the necessary information and documents, which shall be registered and stored, in order to identify him and carry out a due diligence, defined by this Regulation.

8.2 The calculation is performed in such a way that, if necessary, it is possible to recover the data of the employee who performed the due diligence of the Client or other actions aimed at obtaining the information and documents to be preserved.

8.3 The employees who establish direct contact with the Client and the ICU ensure the security and confidentiality of the stored information and documents.

8.4 Information (including documents) is recorded and stored in paper and/or electronic form for at least 5 years after the termination of the Business Relationship or execution of the Transaction, and for a longer period if provided by the legislation governing the securities market.

8.5 The information to be stored and recorded is:

8.5.1 The contract concluded with the Client,

8.5.2 The information provided by the Client (documents),

8.5.3 The electronic communications between the Client and the Company (if any);

8.5.4 Information about the Client is collected by the responsible employees of the Internal Compliance Unit and not provided for in the previous clauses.

CHAPTER 9: EMPLOYEES TRAINING

9.1. The Company shall organize regular training on the prevention of money laundering and terrorist financing for the Executive Director, the responsible employees of the Internal Compliance Unit, the Company's employees and the persons performing Internal Audit functions.

9.2. Anti-ML/AF trainings shall be held by the responsible employee of the Internal Compliance Unit at least twice a year, within 20 /twenty/ working days from the moment of submission of the report provided for in sub-clause 3. 7 of the Regulation. The training schedule is approved by the Company's Executive Director, taking into account the workload and work schedule of the Company's employees. Anti-ML/AF trainings are organized for new employees within three months after they have started working.

9.3. The training schedule is included in the report submitted by the responsible employee of the Internal Compliance Unit.

9.4. Anti-money laundering and anti-terrorist financing trainings are recorded by the responsible employee of the Internal Compliance Unit.

9.5. The implemented training materials, the information about the employees who participated in it and the documents certifying the participation are recorded (Appendix 6) and stored for at least 5 years.

CHAPTER 10. MONITORING, RESPONSIBILITY AND IMPLEMENTATION OF INTERNAL AUDIT REGARDING COMPLIANCE WITH REGULATORY REQUIREMENTS

- 10.1.** The control over the fulfillment of the requirements of the regulation is carried out by the Internal Compliance Unit.
- 10.2.** The internal auditor conducts inspections at least once a year in accordance with the procedure established by the Law to make sure that the Executive Director and the Internal Compliance Unit ensure full compliance of the Company's activities with the requirements of the Law, normative legal acts of the Authorized Body and other internal legal acts.
- 10.3.** The internal auditor shall report to the Executive Director and the Assembly on his assessments and findings from the audits, including his conclusion on the adequacy and effectiveness of employees' training on the prevention of money laundering and terrorist financing.
- 10.4.** In case of discovery of suspicious transactions or potential money laundering schemes, violations of requirements of the Law and other legal acts adopted on its basis (internal and external) during the current or planned inspection, the internal auditor shall inform the Internal Compliance Unit before submitting the document on the results of the inspection to the relevant competent authority in order to implement the necessary measures to combat money laundering and terrorist financing.
- 10.5.** The relevant employees providing direct contact with the Client and the ICU shall take the responsibility for non-fulfillment or improper implementation of the duties and responsibilities defined by the Regulation, organizing and ensuring the defined functions/steps, collecting and maintaining the required information.
- 10.6.** Responsibilities defined by the regulation shall be carried out by the responsible employees of the ICU.
- 10.7.** The ICU is responsible for the coordination of ML/TF prevention functions in the Company and the current control over their proper implementation. The control over the requirements established by the Regulation shall be carried out by the Internal Audit.

CHAPTER 11. FINAL PROVISIONS

- 11.1** All additions and amendments to these Regulations are approved by the Executive Director of the Company (unless otherwise provided by the Company's Charter) and enter into force upon approval by the Executive Director.