Approved by the Shareholders' meeting of
"Invia Investments" CJSC
Dated on 27/11/2023

Executive Director of "Invia Investments" CJSC
Anahit Shakaryan

"Invia Investments"

Closed Joint Stock Company

RULES FOR PREVENTION OF MONEY LAUNDERING AND TERRORISM FINANCING

(new edition)

Contents

The rules for prevention of money laundering and terrorist financing of “Invia Investments” closed joint stock company (hereinafter referred to as “the Company”) have been drawn up in accordance with the legislation regulating the securities market of the Republic of Armenia, the Law of the Republic of Armenia “On Combating Money Laundering and Terrorism Financing" (hereinafter referred to as “the Law”), the normative legal acts adopted by the Central Bank of the Republic of Armenia and the Company's charter and regulate the procedures for the prevention of money laundering and terrorist financing through the Company.

1. GENERAL TERMS

1.1. The terms used in these rules are interpreted in the sense of the terms defined by the Law.

2. INTERNAL MONITORING UNIT

2.1. The function of internal monitoring unit is carried out by the internal audit department of the Company, in accordance with the procedures defined by the "regulations of the internal audit department" of the Company.

2.2. The internal monitoring unit of the Company is independent in carrying out the functions defined under the Law and regulations adopted on the basis thereof and shall have the status of senior management of the Company.

2.3. The internal monitoring unit:

- 2.3.1. ensures the submission of information on behalf of the Company to the authorized body, as well as the Company's communication with the authorized body;
- 2.3.2. conducts analyses to identify suspicious transactions or business relationships;
- 2.3.3. preserves the findings of the analyses conducted for identifying suspicious transactions or business relationships;
- 2.3.4. ensures risk assessment of clients and transactions or business relationships;
- 2.3.5. whenever necessary, discusses with the respective employee who provided the internal impulse, the issue of recognizing a transaction or a business relationship as suspicious, suspending, rejecting or terminating the implementation thereof, or freezing the property of persons associated with terrorism;
- 2.3.6. makes a final decision on recognizing a transaction or a business relationship as suspicious, suspending, rejecting, or terminating the implementation thereof, or freezing the property of persons associated with terrorism;
- 2.3.7. carries out other functions as defined by the Law, these Rules and other legal acts adopted on the basis of the Law.

2.4. The internal monitoring unit may:

- 2.4.1. develop internal legal acts, submit them to the CEO of the Company for approval;
- 2.4.2. monitor the effectiveness of internal legal acts; make proposals on their improvement;
- 2.4.3. carry out other functions as assigned by the CEO, insofar as it does not restrict the independence of the internal monitoring unit.

2.5. In performing its functions aimed at prevention of money laundering and terrorism financing the internal monitoring unit shall provide support and advice to the other employees of the Company who are competent in the field of prevention of money laundering and terrorism financing.

2.6. The internal monitoring unit is entitled to directly present the issues arising in relation to the prevention of money laundering and terrorism financing to the Board of Directors of the Company (the competent body if no Board of Directors is formed in the Company), as well as to participate in discussions held by the Board of Directors (another competent body if no Board of Directors is formed in the Company) on matters related to the prevention of money laundering and terrorism financing.

2.7. The internal monitoring unit shall periodically, but no later than once every six months, examine the compliance of the Company's transactions and business relationships, structural divisions and employees' actions with the Law and the legal acts adopted on the basis thereof. The internal monitoring unit submits a report to the Board of Directors of the Company (another competent body if no Board of Directors is formed in the Company) on the results of the examination, as well as on other issues raised by the authorized body.

2.8. The report on the results of the examination defined in the point 2.7. shall include at least:

2.8.1. the number of transactions subject to mandatory notification, the number and brief description of suspicious transactions and business relationships,

2.8.2. the number and summary description of the transactions and business relationships that were analyzed but were not qualified as suspicious;

2.8.3. the number and brief description of transactions and business relationships suspended, rejected or terminated by the Company, the value of each suspended transaction or business relationship,

2.8.4. amount of frozen property,

2.8.5. Cases of violations of the requirements of the Law, these rules and other legal acts adopted on the basis of the Law as a result of the actions of the Company's employees.

2.9. The internal monitoring unit can inform the executive body about its decision to qualify the transaction or business relationship as suspicious, to suspend, reject or terminate the implementation thereof, to freeze the property of persons associated with terrorism, only after providing the report on the suspicious transaction or business relationship to the authorized body, after making a decision on suspending, rejecting or terminating the implementation of the transaction or business relationship, freezing the financial means or other asset of persons associated with terrorism.

2.10. The internal monitoring unit and client service departments or employees shall cooperate at all times by carrying out the following activities:

2.10.1. the internal monitoring unit shall periodically organize trainings and seminars for client service departments or employees, introducing them to the latest news, including typologies, in the field of combat against money laundering and terrorism financing;

2.10.2. the internal monitoring unit shall provide at all times client service departments or employees with the latest lists of non-cooperating countries or persons associated with terrorism published by the United Nations Organization or authorized body;

2.10.3. client service departments or employees must provide the internal monitoring unit at its first request with any documents in their possession and any information known to them regarding clients, their transactions and business relationships;

2.10.4. client service departments or employees shall comply with the obligations imposed in them by clauses 7.7, 11.5 and 11.6 of these rules.

3. RECRUITMENT, TRAINING AND EDUCATION OF EMPLOYEES OF INTERNAL MONITORING UNIT AND OTHER EMPLOYEES

3.1. The recruitment process for the employees of the internal monitoring unit is carried out in accordance with the Company's "Regulations of the Internal Audit Department" and "Internal Labor Disciplinary Rules", and other employees related to the prevention of money laundering and terrorism financing are recruited in accordance with the "Internal Labor Disciplinary Rules".

3.2. To properly perform the functions outlined by the Law, these rules, and other legal acts adopted on the basis of the Law, the employee of the internal monitoring unit of the Company shall hold a higher education degree or a recognized professional (in the financial sector) qualification certificate from the Republic of Armenia or internationally recognized institutions and have accumulated a minimum of one year of work experience, within the past ten years, either in the financial sector or in the domain of combating money laundering and terrorism financing.

3.3. The employee of the internal monitoring unit cannot be a person who, in accordance with the law:

3.3.1. has been convicted of an intentional crime;

3.3.2. has been legally deprived by a court of the right to hold positions in the financial, banking, tax, customs, commercial, economic, or legal fields;
3.3.3. has been declared bankrupt and has outstanding (unforgiven) obligations.
3.3.4. is a suspect, accused, or involved in a criminal case under investigation by law enforcement authorities in the Republic of Armenia or other states.
3.3.5. does not meet the criteria specified in point 3.2 of these rules.

3.4. The information provided by points 3.2 and 3.3 of these rules is submitted by the declaration "Regarding the employee of the internal monitoring unit" defined by the authorized body (hereinafter referred to as "the Declaration"), which is submitted to the Company before being appointed to the position of employee of the internal monitoring unit. The reliability of the information presented in the declaration can be checked in any lawful way not prohibited by law.

3.5. All employees within the Company who are involved in activities related to the prevention of money laundering and terrorism financing shall be aware of the anti-money laundering and anti-terrorism financing legislation, along with other relevant legal acts (especially regarding client due diligence and regarding obligations on reporting a suspicious business relationship or transaction regarding reporting obligations), as well as existing risks and typologies associated with money laundering and terrorism financing.

3.6. To meet the requirement stated in point 3.5, the Company shall conduct regular training sessions for the board members, executive body, internal monitoring unit, client service representatives, internal audit personnel, as well as for other relevant employees involved in the prevention of money laundering and terrorism financing, on the subject of preventing money laundering and terrorism financing.

3.7. The training session on the subject of preventing money laundering and terrorism financing provided for in the point 3.6 for the new employees shall be conducted within three months of their employment.

3.8. The training materials implemented by the Company, the data of the employees who participated in them and the documents certifying the participation shall be recorded and kept for at least 5 years.

4. RISK MANAGEMENT

4.1. Risk management in the company is carried out in the following two stages:
4.1.1. Risk assessment
4.1.2. Implementation of risk mitigation measures

4.2. The risk may be assessed as medium (standard), high, or low. The risk shall be assessed on the basis of the specific criterion characterizing the given risk, whereas in the presence of more than one criterion it shall be determined by combination thereof. The criteria of risk are defined by the Law, these Rules, and other legal acts adopted on the basis of the Law.

4.3. The risk shall be assessed as medium (standard) whenever the criteria of high or low risk are absent, except for the case provided for in point 4.5.2 of these rules.

4.4. The risk shall be assessed as high whenever at least one criterion of high risk is present, except for the case provided for in point 4.5.3. of these rules.

4.5. The risk shall be assessed as low whenever:
4.5.1. only criteria of low risk are present;
4.5.2. a medium (standard) risk criterion is present, but the transaction in question is a low-risk transaction stipulated under point 4.9 of these Rules;
4.5.3. a high-risk criterion is present, but the transaction in question is a low-risk transaction stipulated under point 4.9 of these Rules

4.6. In case of simultaneous presence of several criteria for different risks, the risk shall be assessed by the higher risk criterion, except for the cases stipulated under sub-points 4.5.2 and 4.5.3 of these rules.

4.7. In the event that any new risk criteria emerge during the course of the business relationship with the client, the Company shall review the assessment of the given risk by conducting appropriate due diligence measures on the client that align with the newly identified risk factors.

4.8. The criteria of high risk are:

- 4.8.1. legal entities or organizations whose field of activity is individual management of assets,
- 4.8.2. Companies have nominal shareholders or with bearer shares;
- 4.8.3. Businesses and business relationships characterized by large-scale use of cash;
- 4.8.4. Companies that have unusual or excessively complex ownership structure;
- 4.8.5. provision of personalized banking services,
- 4.8.6. transactions or business relationship without face-to-face contact;
- 4.8.7. Potential or existing clients or real beneficiaries who are politically exposed persons, members of their families (parents, spouse, grandparents, siblings, children, in-laws) or persons otherwise associated with them;
- 4.8.8. persons (including financial institutions) that are domiciled or reside in non-cooperative countries or territories, or come from such countries or territories;
- 4.8.9. the clients whose accounts are used to make frequent and inexplicable transfers to various financial institutions;
- 4.8.10. The clients whose transaction and/or business relationships structure or nature make it difficult to identify the real beneficiary;
- 4.8.11. The clients carrying out cash-based activities, including: clients providing money services (e.g. money transfer organizations, exchange offices), casinos, entities organizing games of chance, or clients whose activities are not usually cash-based, but for certain transaction they use large amounts of cash;
- 4.8.12. non-profit organizations;
- 4.8.13. accountants, lawyers, or other specialized persons carrying out similar activities that are served by financial institutions and act on behalf of their clients;
- 4.8.14. intermediaries (financial and non-financial) whose activities are not regulated by the legislation on combating money laundering and terrorism financing;
- 4.8.15. the clients using bearer securities, including bearer cheque books;
- 4.8.16. all complicated or unusually large transactions, as well as transactions or business relationships involving unusual conditions lacking obvious economic or other legal purposes.

4.9. The criteria of low risk are:

- 4.9.1. Payments made to the state or community budgets of the Republic of Armenia;
- 4.9.2. Financial institutions that are effectively supervised in terms of money laundering and terrorism financing prevention;
- 4.9.3. state bodies; local self-government bodies; state non-profit organizations; state administrative institutions except for bodies or organizations located in non-cooperative countries or territories.

4.10. In applying a risk-based approach, the Company takes into account risk factors that are specific to an individual client or transaction and may affect the determination of the assumed level of risks for them. They include:

- 4.10.1. due to the client's identity, his business profile;
- 4.10.2. the purpose of the client's account or the nature of business relationship;
- 4.10.3. the amount of funds invested into the account by a specific client or the amount of the transaction carried out;
- 4.10.4. the regulatory, management or supervisory system under which the client financial institution operates;
- 4.10.5. duration and regularity of the business relationship;
- 4.10.6. familiarity with the country, which includes knowledge of the country's laws, regulations and rules;

4.10.7. the use of intermediary legal entities or structures that do not have an obvious economic purpose or other logical justification or unnecessarily complicate the transaction/business relationship and lead to a lack of transparency.

4.11. For the purposes of risk management, the following procedures are used in the Company:

4.11.1. Timely identification and verification of identity of each client;

4.11.2. taking the necessary measures to find out the existence of the real beneficiary, and in case of existence, identification and identity verification of the latter;

4.11.3. if an authorized person acts on behalf of the client, then also identification of that person, verification of identity and authority to act on behalf of the client,

4.11.4. obtaining information necessary to understand the client's financial condition and trading activity, including the expected scope and nature of transactions.

4.12. When introducing new services, adopting new methods of providing them, or utilizing emerging technologies, with the aim of mitigating potential and existing risks, the procedures for introducing these new services, methods of providing them or utilizing the technologies shall be discussed with the internal monitoring unit and implemented only upon receiving a positive opinion of the internal monitoring unit.

4.13. For the purpose of effective risk management, when establishing a business relationship or concluding a transaction without face-to-face contact, the Company shall:

4.13.1. ensure that the required documents and orders are submitted by the client using a valid email address, electronic signature or code mechanism.

4.13.2. Within the due diligence of the client, demand the payments to be made to an account held in the name of the customer at a financial institution that satisfies the requirements outlined in subparagraphs "a" to "c" of paragraph 3 of part 8 of Article 16 of the Law.

5. CLIENT DUE DILIGENCE (INCLUDING ENHANCED AND SIMPLIFIED) AND RETENTION OF INFORMATION

5.1. With exception to the case specified in the point 5.34 of these rules, the Company shall carry out client due diligence when:

5.1.1. Business relationship is being established;

5.1.2. An occasional transaction (interlinked occasional transactions) is being carried out with value equal to or exceeding AMD 400,000 (four hundred thousand drams), unless a stricter provision is provided in the Law;

5.1.3. Suspicions arise with regard to the reliability or completeness of previously obtained client identification data (including documents);

5.1.4. Suspicions arise with regard to money laundering or terrorism financing.

5.2. The client due diligence process includes identifying and verifying the client (including authorized person and beneficial owner), determining the purpose and intended nature of the business relationship, and throughout the course of the business relationship (including the moment of establishing a business relationship with the client) conducting ongoing due diligence.

5.3. The Company shall perform client due diligence in two stages:

5.3.1. Obtaining documents and information from the client;

5.3.2. Reviewing the documents and information obtained from the client (if necessary, also from other sources) and determining the client’s business profile.

5.4. The first stage of client due diligence shall be carried out by the Company’s client service employees, while the second stage shall be carried out by the internal monitoring unit.

5.5. The Company can initiate a business relationship or carry out an occasional transaction with the client only upon receipt and verification of the specified information (including documents) specified in these rules for client identification. The Company has the option to verify the client's identity based on the

necessary identification information stipulated in these rules when establishing a business relationship or conducting an occasional transaction, or after it within a reasonable timeframe, not exceeding seven days, if it is necessary to ensure smooth business interactions with the client, provided that a Company manager or an employee directly serving the client knows the client personally and can assure that all mandatory documents and information will be furnished by the client.

5.6. During the client identification process, the Company shall ascertain whether the client is acting in their individual capacity, on behalf of another individual, or on behalf of an entity, as well as

5.6.1. find out the presence of an authorized person and, if present, in accordance with these rules, identify the authorized person, verify his identity and his authority to act on behalf of the client,

5.6.2. find out the existence of the ultimate beneficial owner and, if present, in accordance with these rules, identify the beneficial owner and verify his identity.

5.7. In the case of clients who are legal entities, for the purposes of identifying the ultimate beneficial owner the Company shall possess comprehensive information regarding the authorities held by the participants and management bodies of the given legal entity.

5.8. The Company conducts client identification and verifies their identity using credible and valid documents, as well as other information obtained from competent state authorities and specialized organizations with relevant expertise.

5.9. To identify a natural person client, authorized person, or beneficial owner, the Company shall request the following documents from the client:

5.9.1. A copy of the client's identity document.

5.9.2. If the client is an individual entrepreneur, the copies of the document(s) that contain the registration number, Taxpayer Identification Number (TIN), or any other equivalent numbers associated with the individual entrepreneur's business.

5.9.3. declaration on the existence (absence) of the beneficial owner in the form established by the authorized body,

5.9.4. A statement about the center of vital interests, if the client is a foreign person and the center of their vital interests is not indicated in any other document,

5.9.5. Any other document required by any internal legal act of the Company,

5.9.6. Any other document that may be required by the internal monitoring unit.

5.10. To identify a client or authorized person as a legal entity, the Company shall request the following documents from the client:

5.10.1. Copy of the most recent version of the document certifying the state registration of the legal entity;

5.10.2. Copy of the document containing taxpayer identification number (TIN) or other equivalent number,

5.10.3. Copy of the most recent version of incorporation documents.

5.10.4. List of natural persons who are authorized to act on behalf of the client without a power of attorney and copies of documents certifying their appointment,

5.10.5. List of natural persons who are authorized to act on behalf of the client on the basis of a power of attorney and the documents certifying their powers or the copies thereof,

5.10.6. Declaration on the existence or absence of a beneficial owner, in the form established by the authorized body.

5.10.7. For individuals specified in points 5.10.4 - 5.10.6 of these rules, the required documents outlined in point 5.9 of these rules, with the exception of point 5.9.3.

5.10.8. List of persons who own twenty percent or more of the client’s equity securities

5.10.9. A statement about the center of vital interests, if the client is a foreign person and the center of their vital interests is not indicated in any other document,

5.10.10. Any other document required by any internal legal act of the Company

5.10.11. Any other document that may be required by the internal monitoring unit

5.11. In order to identify the client or authorized person as a state body or local self-government body, the Company shall request the following documents:

5.11.1. The full official name of the state body or local self-government body, along with a letter indicating the country.

5.11.2. Any other document required by any internal legal act of the Company

5.11.3. Any other document that may be required by the internal monitoring unit

5.12. Based on the documents specified in points 5.9 - 5.11 of these rules, the internal monitoring unit conducts a risk assessment of the client and the transaction or business relationship established with them. Based on this assessment, the internal monitoring unit determines whether to apply simplified, enhanced, or standard due diligence procedures.

5.12.1. Account is opened for an individual when the client provides the documents mentioned in points 5.9.1-5.9.6 and responsible employees or the implemented online system perform verification checks. After successful verification, the client gets access to his account, where he can carry out transactions in the amount of a maximum of AMD 400,000.

5.12.2. To perform transactions exceeding AMD 400,000 the Client shall provide additional proof of residency/registration document (registration details from the passport, reference from the bank, utility bills, etc.). After the check of the document the client can perform transactions of amount up to AMD 2 million.

5.12.3. In order to carry out transactions exceeding AMD 2 million, the client must submit additional documents regarding the origin of the funds (reference from the workplace, bank statement, sales contract and other documents). After verification of documents and a positive conclusion, the client can carry out transactions on his account that exceed AMD 2 million.

5.12.4. In case of risk indicators, the employee of the internal monitoring body has the right to request additional documents and, if necessary, can block the client's account.

5.13. In cases where the client poses a medium (standard) level of risk, the Company follows the due diligence process as outlined in Clause 19 of Article 3, Part 1 of the Law. This involves fulfilling the requirements specified in that clause and other relevant provisions of the Law, as well as conducting regular ongoing due diligence on the business relationship.

5.14. In order to observe transactions with the client within the framework of the ongoing due diligence of the business relationship provided for by Article 17, Part 1 of the Law, the Company undertakes the following measures in case of medium (standard) risk:

5.14.1. Verifies the authenticity and reliability of the information (including documents) required from the client in connection with the transaction or business relationship, using, if necessary, the limited availability of information (World-check system or any other similar system, which will not be inferior to World-check in terms of its distribution and databases); and from publicly available sources, making inquiries to competent authorities and other reporting entities, as well as foreign partners,

5.14.2. identifies connections between clients, transactions and business relationships; compares the sources, movement and volumes of the client's working capital in different transactions during the unit period only when they exceed the reasonable monetary limit from the point of view of the client's business characteristics.

5.15. If the risk is determined to be high, the Company conducts enhanced due diligence on the client following the procedure outlined in Article 3, Part 1, Clause 22 of the Law, within which the Company, in fulfillment of the requirements set by that clause and other relevant provisions of the Law, in case of high risk, carries out enhanced measure of the ongoing due diligence of the business relationship, if needed additional documents are requested.

5.16. To effectively monitor transactions with the client as part of the ongoing due diligence of the business relationship provided in Article 17, Part 1 of the Law, the Company implements the following enhanced measures in case of high-risk:

5.16.1. when checking the authenticity and reliability of information (including documents) required from the client in relation to a transaction or business relationship, requests necessary information (including additional documents), uses limited access to information (World-check system or any other similar system, which will not be inferior to World-check in terms of its distribution and databases) and from publicly available sources, makes inquiries to the largest possible number of competent authorities and other reporting persons, as well as foreign partners,

5.16.2. When comparing the sources, movements, and quantities of the client's working capital involved in various transactions, the Company selects the longest possible period or multiple comparable unit periods.

5.16.3. when determining the existence of connections between clients, transactions and business relationships, performs a multi-level analysis of them, including 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, requires information (including documents) fully justifying the actions performed within them,

5.16.5. when determining the source of the client's income and assets, requires information (including documents) that substantiates their legality.

5.17. In cases of low risk, the company may conduct a simplified due diligence process as defined in Section 3, Part 1, Clause 24 of the Law, within which the Company, in compliance with the requirements set forth in that clause and other relevant provisions of the Law in case of low risk, may implement reduced measures of ongoing due diligence of the business relationship.

5.18. To effectively monitor transactions with the client as part of the ongoing due diligence of the business relationship outlined in Section 17, Part 1, Clause 1 of the Law, the Company implements the following reduced measures in case of low-risk:

5.18.1. Verify the authenticity and reliability of information (including documents) required from the client regarding the nature and legitimacy of the transaction or business relationship, based on the information provided by the client.

5.18.2. Compare the sources, movement, and volumes of working capital involved in different transactions carried out during a certain period of time by the client to determine the origins of those funds only when they exceed the monetary threshold specified in the client's transaction profile.

5.18.3. Identify connections between clients, transactions, and business relationships only in cases where there is evidence of relationships between clients with medium (standard) or high-risk clients, transactions, or business relationships.

5.19. According to Article 17, Part 1 of the Law, ongoing monitoring of the business relationship of a client conducting a business transaction is carried out throughout the entire process (including establishing the client's approval of the business transaction), within which the measure outlined in points 5.14.1, 5.14.2, 5.14.3, 5.18.2, and 5.18.3 of these rules shall be implemented, not later than:

5.19.1 Once a year in the case of low and medium (standard) risk.

5.19.2 Once every six months in the case of high risk, excluding the case provided for in point 5.23 of these rules.

5.20. According to Article 17, Part 2 of the Law, the update of the collected information during the client's ongoing due diligence (including the verification of the client's identity and the information obtained in the verification process) shall be carried out not later than:

5.20.1. Once a year in the case of medium (standard) risk and low risk.

5.20.2. Once every six months in the case of high risk, excluding the case provided for in point 5.23 of these rules.

5.21. The update of the information obtained during the client's identification and verification process is carried out once a year.

5.22. The requirements of regulatory compliance, including the need to conduct due diligence on existing clients, are implemented by conducting periodic reviews and monitoring of the financing of terrorism risks, in accordance with the following cases and deadlines.

5.22.1. For the purposes of identifying and verifying the identity of the client (including the authorized person and the beneficial owner), as well as to clarify the purpose of the business relationship and the intended nature of the transaction, the new requirements should be met before the first transaction with the client or when updating the information collected during the client's periodic review, as specified in point 5.20 of these rules, provided that no transaction has been conducted with the client since the last update.

5.22.2. For ongoing due diligence of the client's business relationship from the moment the new requirements take effect.

5.23. In the case of politically exposed persons, the ongoing additional monitoring specified in clause 22 of part 1 of Article 3 of the Law shall include the measures envisaged in the point 5.16 of these rules, the implementation of which shall be at least every three months, in accordance with the provisions of points 5.19 and 5.20 of these rules.

5.24. The statement regarding the presence (absence) of the beneficial owner submitted by the client during the business relationship must also be completed when a beneficial owner appears or when the beneficial owner changes.

5.25. When performing the actions described in subparagraphs "a" and "b" of Article 3, Part 1, Clause 19 of the Law, the Company may rely on data obtained through the client's due diligence conducted by another financial institution, non-financial institution, or individual, provided that the following conditions are met:

5.25.1. The Company promptly obtains the relevant information from another financial institution, non-financial institution, or individual.

5.25.2. The Company takes adequate measures to ensure that the other financial institution, non-financial institution, or individual:

5.25.2.1. Is authorized and capable of immediately providing, upon request, the information obtained through cleint due diligence, including document copies.

5.25.2.2. The other financial institution, non-financial institution, or individual, in terms of anti-money laundering and combating the financing of terrorism, must be subject to appropriate regulation and supervision, and have effective procedures for client due diligence and information retention as prescribed by the Law and related legal acts.

5.25.2.3. The other financial institution, non-financial institution, or individual must not be located or registered in a jurisdiction or territory that is considered non-compliant, nor be associated with a jurisdiction or territory that is considered non-compliant.

5.26. For the purposes of client due diligence, the documents and information provided by the client may be in Armenian, Russian, or English. However, if documents are submitted in a language other than these languages, they must be notarized and translated into Armenian.

5.27. If foreign individuals submit documents in a language other than Armenian, those documents must be accompanied by an apostille or consular certification, unless the Company has an agreement allowing submission without an apostille or consular certification.

5.28. In the course of establishing correspondent or similar relationships with foreign financial institutions, in addition to complying with the requirements specified by the Law and these rules for client due diligence, the Company shall:

5.28.1. Gather sufficient information to fully understand the nature of the reporting institution's activities and assess the business reputation of the reporting institution and the effectiveness of its control systems, based on public and other reliable information, including whether the financial institution has been or is currently involved in money laundering or terrorism financing as part of a criminal investigation or any other related proceeding.

5.28.2. Evaluate the adequacy and effectiveness of the correspondent institution's anti-money laundering and anti-terrorist financing procedures.

5.28.3. Obtain approval from senior management prior to establishing a correspondent or similar relationship.

5.28.4. document the respective anti-money laundering and anti-terrorism financing responsibilities of each reporting institution, if not clearly known;

5.28.5. ensure that in the case of transit accounts, the correspondent institution:

5.28.5.1. has conducted due diligence on clients with direct access to the accounts of the financial institution and can provide the necessary due diligence information on those clients upon request,

5.28.5.2. does not allow fraudulent banks to use its accounts.

5.29. The Company must retain the information obtained during the client due diligence process, including the documents, as required by the Law and these rules, whether the transaction or business relationship continues or is terminated, including

5.29.1. client identification data, including account number and account transaction data, as well as business correspondence data,

5.29.2. all necessary data regarding domestic and international transactions or business relationships (including the name of the customer (and the other party to the transaction), registration address (if available) and place of residence (location), nature of the transaction, execution period, amount and currency, if available also: account type and account number) that will be sufficient to restore a complete picture of the given transaction or business relationship,

5.29.3. Information on suspicious transactions or business relationships provided for in Article 7 of the Law, as well as information on the process (analysis performed) and results of the observation of suspicious transactions or business relationships not recognized as suspicious,

5.29.4. The results of the assessment of the actual and potential risks of financing of terrorism and money laundering risks, as envisaged in Article 4 of the Law.

5.29.5. Other information defined by the Law and these rules.

5.30. The information specified in point 5.29 (including documents) must be kept for at least 5 years from the completion of the transaction or the performance of the transaction, and in the case of a provision stipulated by the law, for a longer period.

5.31. The information (including documents) required by the Law and maintained by the Company must be sufficient for a comprehensive and accurate provision of information requested by the competent bodies, bodies implementing a criminal prosecution in cases prescribed by the law, regarding clients, transactions, or business relationships.

5.32. The information specified by the law and these rules, including documents, can be collected and retained in paper or electronic form.

5.33. The retention of mandatory information specified by the Law and these rules, including documents, must be registered. The registration should be done in a way that allows the retrieval of employee data if necessary, who conducted the client's research or the retention of mandatory information (including documents) in case of other relevant actions.

5.34. The procedures defined by the Law and these rules for conducting client due diligence are not applied in cases of transactions performed by the Company for its own needs in order to ensure its current activities (except for purchases of financial assets).

5.35. If the client fails to provide the Company with the information required in points 5.20-5.21 of these rules within the specified timeframe set by the Company, the Company has the right to suspend the provision of services to the client until the required information is provided.

5.36. When conducting client due diligence, the Company shall also guided by the following guidelines:

5.36.1. Prior to opening an account for each client, the client’s package of documents must be checked by the internal monitoring unit and the account must be opened only if the latter's positive conclusion is reached.

5.36.2. Prior to the implementation of the online system for opening accounts for individuals, identification and due diligence of all client must be done with human involvement. Alongside the implementation of the online account opening system, customers should also be introduced an automated and human-free identification and identity document verification system from an organization with extensive experience in the field.

5.36.3. The Company's existing client base should be subjected to periodic inspections by the internal monitoring unit, which can be carried out both manually and by the introduction of automated systems, and the Company should take measures to implement such automation systems that will allow to synchronize the Company's client base with listings of local and international unwanted persons and increase the frequency of inspections to the point of continuity.

5.36.4. The Company shall also take measures to implement such automated systems that will allow for periodic monitoring and comparison of client transactions with the clients' business characteristics and previous transactions, to identify transactions with significant deviations and make them the subject of a more detailed study.

5.36.5. The Company shall use all available means and sources, including information obtained from other financial institutions, to verify the legitimacy of the Client's funds.

5.36.6. The employee of the internal monitoring body should periodically conduct sample checks on automatically opened accounts, request additional documents from clients if necessary, and in case of suspicious and risk indicators, may change the risk class, limits of services provided, if necessary, may also block the client's account and suspend the provision of services.

6. COLLECTION, REGISTRATION AND RETENTION OF INFORMATION ON TRANSACTIONS AND BUSINESS RELATIONSHIPS

6.1. Collection and registration of information about transactions and business relationships shall be implemented by the employees directly involved in client service or directly conducting the transactions, and, if necessary, by the staff of internal monitoring unit.

6.2. Collection of information about transactions or business relationships may be implemented in both paper or electronic ways.

6.3. Information about transactions or business relationships is registered in information databases maintained by the Company or permanently available to the Company.

6.4. The requirements of clauses 5.30 - 5.34 of these rules apply to the retention of information about transactions or business relations.

7. RECOGNIZING A TRANSACTION OR A BUSINESS RELATIONSHIP AS SUSPICIOUS

7.1. The Company shall recognize a transaction or business relationship, including an attempted transaction or business relationship, as suspicious and submit a report on suspicious transaction or business relationship to the authorized body as stipulated under Article 8 of the Law, if it is suspected or there are reasonable grounds to suspect that the property involved in the transaction or business relationship is the proceeds of a criminal activity or is related to terrorism, terrorist acts, terrorist organizations or individual terrorists, or to those who finance terrorism, or was used in or is intended to be used for terrorism, or by terrorist organizations or individual terrorists, or by those who finance terrorism.

7.2. The Company shall consider recognizing a transaction or business relationship as suspicious and submitting a report on suspicious transaction or business relationship to the authorized body as stipulated under Article 8 of the Law, if the circumstances of the case under consideration fully or partially match

the criteria or typologies of suspicious transactions or business relationships, or if it becomes apparent to the Company that, although the suspiciousness of the concluded or proposed transaction or business relationship does not arise from the criteria or typologies of a suspicious transaction or business relationship, the logic, of its execution, the pattern (dynamics) of or other circumstances give the grounds to assume that it may be carried out for the purpose of money laundering or terrorism financing.

7.3. In cases specified under point 7.2 of these Rules, if adequate consideration does not result in recognizing a transaction or business relationship as suspicious and submitting a report on suspicious transaction or business relationship to the authorized body as stipulated under Article 8 of the Law, then the justifications for non-recognition of the transaction or business relationship as suspicious, the conclusions made, the process of analysis and its findings shall be documented and sretained in the manner and timeframe established by the Law.

7.4. The process of recognizing a transaction or a business relationship as suspicious shall be implemented by the Internal monitoring unit pursuant to the provisions of the Law, these Rules and other legal acts adopted on the basis of the Law.

7.5. The process of recognizing a transaction or a business relationship as suspicious commences both upon receiving internal or external signals, as well as upon the initiative of the Internal monitoring unit, when:

7.5.1. There is a potential match of the data on a client or on the other party to a transaction with the identification data of the persons associated with terrorism or other persons specified in the instructions of the authorized body;

7.5.2. The circumstances of the case under consideration fully or partially match the criteria or typologies of suspicious transactions or business relationships;

7.5.3. The logic, pattern (dynamics) of implementation or other characteristics of the concluded or attempted transaction or business relationship give the grounds to assume that it may be carried out for the purpose of money laundering or terrorism financing.

7.6. Internal signals shall be those received from the employees of the client service department, the management bodies of the Company, the internal audit, as well as from other employees with competencies in the prevention of money laundering and terrorism financing, which are transmitted to the Internal monitoring unit in the manner and timeframes established by internal regulations.

7.7. Internal signals shall be transmitted to the Internal monitoring unit by the end of the business day, during which they emerge.

7.8. Internal signals may be transmitted to the Internal monitoring unit verbally or in writing by any means of communication.

7.9. External signals shall be those received from the authorized body, competent bodies, other reporting persons, foreign counterparts, as well as from limited access and publicly available sources of information.

7.10. The Internal monitoring unit shall, in cases specified under sub-point 7.5.1 of these rules, where there is a potential match,

7.10.1. With Identification data of the persons associated with terrorism - immediately conduct matching exercises and, in case of positive match, as well as when the absence of a positive match cannot be reliably ascertained, submit with a report on suspicious transaction or business relationship to the authorized body in the manner established by the Law, and take the measures stipulated under Article 28 of the Law;

7.10.2. Identification data of the persons specified in the assignments of the authorized body — conduct matching exercises within the timeframes specified by the assignments and, in case of positive match, as well as when the absence of a positive match cannot be reliably ascertained, take the actions prescribed by the assignments.

7.11. In cases specified under sub-points 7.5.2 - 7.5.3 of these Rules, the Internal monitoring unit shall within reasonable time conduct comprehensive analyses by using client due diligence information and additionally obtained data, make adjustments in collaboration with the Financial Monitoring Center of the Central Bank of Armenia as necessary and, in case of recognizing the transaction or business relationship

as suspicious, submit a report on suspicious transaction or business relationship to the authorized body in the manner established by the Law, as well as take other measures as stipulated by the Law.

8. SUSPENSION OF A SUSPICIOUS TRANSACTION OR BUSINESS RELATIONSHIP

8.1. In the presence of a suspicion of money laundering or terrorism financing, the Company shall be authorized to suspend the transactions or business relationship for a period of up to five days and immediately submit a report to the authorized body on a suspicious transaction or business relationship as stipulated under Article 8 of the Law.

8.2. In case of having received the assignment specified under Clause 6, Part 1 of Article 10 of the Law, the Company shall suspend the transaction or business relationship for five days and immediately submit a report to the authorized body on a suspicious transaction or business relationship as stipulated under Article 8 of the Law.

8.3. The assignment of the authorized body on suspending a transaction or business relationship shall be implemented immediately upon receipt thereof by the Company.

8.4. In the cases specified under point 8.1 of these Rules, the Internal monitoring unit adopts a decision on suspending a suspicious transaction or business relationship, which necessarily states the period of suspension of transaction or business relationship. The Internal monitoring unit shall notify the Company's executive body about that decision.

8.5. On the basis of the decision of the Internal monitoring unit or the assignment of the authorized body, the employees shall terminate all the actions aimed at continuing the business relationship or conducting a transaction, making a relevant note to this effect in the client record file.

8.6. In the event that the Company does not notify the authorized body about the suspension of the transaction or business relationship, or the authorized body fails to extend the suspension period within 5 days from the moment of suspension of the transaction or business relationship, or the decision of the authorized body to declare the suspension decision void, the decision on suspension is considered void and the suspension is terminated, and an entry is made about it in the client registration register.

8.7. The decision of the Company or the authorized body on suspending a transaction or business relationship may be revoked before the end of the suspension period only by the authorized body upon its own initiative or on the Company’s request, if it is determined that the suspicion of money laundering or terrorism financing is groundless.

8.8. If it turns out that the suspicion of money laundering or financing of terrorism is not founded, the CEO of the Company based on the recommendation of the Internal monitoring unit of the Company submits to the authorized body a request to lift the suspension of the transaction or business relationship before the end of the suspension period.

8.9. On the basis of the request specified in the point 8.8 or on the initiative of the authorized body based on the decision of the authorized body to lift the suspension of the transaction or business relationship before the end of the suspension period, the Internal monitoring unit of the Company makes a decision on lifting the suspension before the end of the suspension period, based on which the suspension shall be terminated, and a relevant note to this effect is made in the client record file.

9. REJECTION OR TERMINATION OF A SUSPICIOUS TRANSACTION OR BUSINESS RELATIONSHIP

9.1. In the event that it is not possible to carry out the duties of client due diligence provided by the Law and these Rules, the Company shall reject the implementation of transaction or business relationship and consider recognizing it as suspicious.

9.2. The Company shall reject the implementation of transaction or business relationship and consider recognizing it as suspicious also in cases of receiving an instruction to reject the implementation of a transaction or business according to subpoint 6, Part 1 of Article 10 of the Law.
9.3. The Internal monitoring unit adopts a written decision on rejection of the transaction or business relationship in the cases specified in point 9.1 of these Rules. The Internal monitoring unit shall inform the Company's executive body about that decision.
9.4. Based on the decision of the Internal monitoring unit or on the assignment of the authorized body the employees shall terminate all the actions aimed at continuing the business relationship or conducting a transaction, and notify the client accordingly.

10. FREEZING OF PROPERTY BELONGING TO PERSONS LINKED TO TERRORISM

10.1. The property owned or controlled directly or indirectly by persons associated with terrorism, by the persons included in the lists published by or in accordance with the United Nations Security Council resolutions, as well as in the lists specified under Part 2 of Article 28 of the Law shall be subject to freezing by the Company without delay and without prior notice to the given persons.
10.2. The property of a client may also be frozen on the basis of the decision of the authorized body.
10.3. In the cases specified in point 10.1 of these rules, the Internal monitoring unit adopts a written decision on freezing the property of a client. The Internal monitoring unit shall inform the Company's executive body about that decision.
10.4. Information about client, its property and freezing thereof based on the decision of the Internal monitoring unit or the authorized body shall be registered in the client's record file.
10.5. Upon freezing of the property of the persons associated with terrorism the Company shall without delay proceed to recognize the transaction or business relationship as suspicious, and to submit a report on suspicious transaction or business relationship.
10.6. The property belonging to bona fide third parties, i.e. the persons who, when transferring the property to another person, did not know or could not have known that it would be used or was intended for use in criminal purposes, including those of terrorism or terrorism financing, as well as the persons who, when acquiring the property, did not know or could not have known that it was the proceeds of a criminal activity, may not be subject to freezing.
10.7. The unfreezing of the property is carried out only by the authorized body, if the property has been frozen by mistake, as well as in case of seizure the frozen property by the prosecuting authority. The freezing of the property of the persons specified under Part 2 of Article 28 of the Law shall also be lifted, if it is established that the person with frozen assets has been removed from the list of persons associated with terrorism.
10.8. Information about the unfreezing shall be registered in the client's record file.

11. SUBMISSION OF REPORTS TO THE AUTHORIZED BODY

11.1. The Company shall submit a report on suspicious transactions or business relationships and (or) on transactions subject to mandatory reporting to the authorized body.
11.2. Reports on suspicious transactions or business relationships are submitted by the Company to the authorized body, regardless of the amounts involved.
11.3. Unless otherwise established by the authorized body, the following transactions are subject to mandatory reporting:
11.3.1. Non-cash transactions with value equal to or exceeding AMD 20 million;
11.3.2. Cash transactions with value equal to or exceeding AMD 5 million.

11.4. The Company, its employees, and representatives are prohibited from informing the person, on whom a report or other information is submitted with the authorized body, as well as other persons, about the fact of submitting such report or other information.

11.5. The client service employee of the Company, in case of discovering suspicions in business relationships or transactions about money laundering and terrorism financing based on the typology or criteria defined by the Law, the guidelines issued by the authorized body, and these Rules, or on his/her own opinion, shall verbally inform the Internal monitoring unit about it till the end of the day of the transaction, while also presenting the grounds and reasons, based on which s/he considers the transaction suspicious. If the client service employee of the Company believes that the transaction shall be suspended or rejected, s/he shall present his/her verbal suggestion to that effect to the Internal monitoring unit before the transaction is conducted.

11.6. If the Company performs a transaction meeting the criteria specified under point 11.3, then the employee who performed that transaction should verbally inform about it the Internal monitoring unit before the end of the day, on which the transaction is performed.

11.7. In the case specified under point 11.6 the Internal monitoring unit within three business days upon receipt of the information shall draw up and submit a report on the transaction to the authorized body in the manner and form established by the authorized body.

11.8. In the case specified under point 11.5 the Internal monitoring unit within one business day upon receipt of the information shall adopt a decision on recognizing or not recognizing the transaction as a suspicious, applying the procedure established under Section 6 of these Rules.

11.9. If as a result of the actions specified under point 11.8 the Internal monitoring unit comes to the conclusion that the transaction is suspicious, it shall submit a report on such transaction within the deadline and in the form and manner established by the authorized body.

12. AUDIT IMPLEMENTATION

12.1. The Company shall perform an internal audit to verify that its activities comply with the provisions of the Law, these rules, and other applicable legal acts adopted on the basis of the Law.

12.2. At least once a year, the executive director of the Company appoints an inspection person or establishes an inspection group that carries out an inspection to verify that both the executive body and the internal monitoring unit ensure the full compliance of the Company with the Law, these rules, and other legal acts adopted on the basis of the Law.

12.3. The group mentioned in point 12.2. shall consist of a minimum of two members who must be employees of the Company, but not members of the executive body, the internal monitoring unit, or individuals directly engaged in the process of client identification and due diligence as specified in this regulation.

12.4. As a result of the implementation of the requirements of point 12.2, the inspection group or person draws up a report, which is submitted to the approval of the executive body of the Company.

12.5. The report drawn up as a result of the implementation of the requirements of point 12.2 shall be duly submitted to the authorized body within one week after the approval of the executive body of the Company.

12.6. While conducting the annual external audit of the Company's financial and economic operations, the auditing organization is also responsible for examining the Company's compliance with the anti-money laundering and anti-terrorism financing legislation, as well as evaluating the effectiveness of its implementation.

12.7. If the authorized body requests an external audit, the Company is required to arrange an external audit within one month. The audit's findings and conclusions shall be submitted to the authorized body within one week after receiving them.

12.8. Upon request, the Company may invite an independent organization to carry out customer data checks according to sanction lists.