RESOLUTION No 22/07-001

OF ARMBROK CHIEF EXECUTIVE OFFICER

on approving the "Rules for Money Laundering and Terrorism Financing Prevention"
of Armbrok ojsc

signed on 28 July 2022

Based on Article 23 of the Law of the Republic of Armenia "On Combating Money Laundering and Preventing Terrorism Financing", sub-point 1 of point 4 and point 6 of the "Regulation on Minimum Requirements to Reporting Entities in the Field of Preventing Money Laundering and Terrorism Financing" approved by the Decision of the Board of the Central Bank of Armenia No 279-N dated 7 October 2014, as well as point 10.15 of the Charter of Armbrok ojsc, I hereby decide that:

1. The new edition of "Rules for Preventing Money Laundering and Terrorism Financing" of Armbrok ojsc attached hereto as Annex 1 be approved.
2. Mr. Hayk Manaselyan, Head of Internal Audit, and Ms. Araksya Harutyunyan, employee of the company, be instructed to advise all Armenbrok ojsc staff members on this Resolution and submit it to the Central Bank of Armenia ojsc by 4 August 2022.
3. Ms. Rouzanna Sarkissian, employee of the company, be instructed to arrange the publishing of this Resolution on the company official website by 4 August 2022.
4. This Resolution shall come into effect upon signing.

Aram Kayfajyan
Chief Executive Officer
"Armbrok" ojsc

Annex 1
to the Resolution No 22/07-001 dd 28 July 2022
of the Chief Executive Officer of Armbrok ojsc

ARMBROK

open joint stock company

RULES FOR MONEY LAUNDERING AND TERRORISM FINANCING PREVENTION

1. Concepts 4
2. Internal monitoring unit 4
3. Hiring, training, and retraining of the internal monitoring unit and other staff 6
4. Risk management....7
5. Customer due diligence (simplified and enhanced) and record keeping 11
6. Collecting, recording, and maintaining of information on transactions and business relationships 18
7. Recognizing a transaction or a business relationship as suspicious 18
8. Suspension of a suspicious transaction or business relationship 20
9. Refusal or termination of a suspicious transaction or business relationship 21
10. Freezing of assets belonging to entities linked to terrorism 21
11. Submission of reports to the authorized body 22
12. Prohibited Activities....23
13. Audit....23

The "Rules for Money Laundering and Terrorism Financing Prevention" (hereinafter: “the Rules”) of "Armbrok” open joint stock company (hereinafter: "the Company") were developed according to the legislation governing the securities market in the Republic of Armenia, the Law of the Republic of Armenia "On Combating Money Laundering and Terrorism Financing" (hereinafter: “the Law”), Central Bank of Armenia regulations, as well as the Company’s Charter and are aimed to define the procedures for preventing money laundering and terrorism financing through the Company.

The Rules must be reviewed to reflect the changes in the Company’s operating environment, but no less than once a year.

1. Concepts

1.1. Concepts used in the Rules shall have the meanings ascribed to them by the Law.

1.2. For the purposes of these Rules, “competent body” shall mean the Board of Directors of the Company, and if such is not appointed then the executive body.

2. Internal monitoring unit

2.1. The Company's internal audit unit shall carry out the responsibilities of the internal monitoring unit, pursuant to the "Regulation of the Internal Audit Unit" of the Company.

2.2. The internal monitoring unit shall be 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.

2.3. The internal monitoring unit shall:

2.3.1. Ensure submission of information on behalf of the Company to the authorized body, as well as provide the connection of the Company with the authorized body;

2.3.2. Conduct analyses to identify suspicious transactions or business relationships;

2.3.3. Maintain the findings of the analyses conducted for detecting suspicious transactions or business relationships;

2.3.4. Ensure risk assessment of customers and transactions or business relationships;

2.3.5. Whenever necessary, discuss with the respective staff member having generated an internal signal the issue of recognizing a transaction or a business relationship as suspicious, suspending, refusing, or terminating it, or freezing the assets of entities linked to terrorism;

2.3.6. Make a final decision on recognizing a transaction or a business relationship as suspicious, suspending, refusing, or terminating them, or freezing the assets of entities linked to terrorism;

2.3.7. Conduct the assessments defined in points 4.2 and 4.3 of the Rules, submit proposals based on the findings thereof to the competent body of the Company.

2.3.8. Review the Rules and, if amendments are deemed necessary, draft and submit them to the competent body of the Company.

2.3.9. Perform other functions as defined by the Law, these Rules and other regulations adopted on the basis of the Law.

2.4. The internal monitoring unit may:

2.4.1. Develop internal regulations, submit them to the Company's executive body for approval;

2.4.2. Monitor the effectiveness of internal regulations; make proposals on their improvement;

2.4.3. Perform other functions as assigned by the executive body, insofar as it does not restrict the independence of the internal monitoring unit.

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

2.6. The internal monitoring unit may directly notify the competent body of the Company of any issues encountered in relation to money laundering and terrorism financing prevention, as well as participate in discussions held by such body on matters related to money laundering and terrorism financing prevention.

2.7. On a regular basis, but no less than once every six months, the internal monitoring unit shall review the transactions carried out and business relationships established by the Company, as well as the activities of the Company's departments and staff to define whether they are in compliance with the Law and regulations adopted based thereon. The internal monitoring unit shall present the report on the findings of the review, as well as other issues raised by the authorized body to the competent body of the Company appointed by the authorized body.

2.8. The report on the findings of the review specified in point 2.7 hereof submitted to the competent body of the Company shall at least comprise:

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

2.8.2. The number and the brief description of the transactions and business relationships, which were analyzed but were not recognized as suspicious;

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

2.8.4. The value of frozen property;

2.8.5. The cases of violating requirements of the Law, these Rules and other legal acts adopted on the basis of the Law due to the actions of staff members of the Company.

2.9. The internal monitoring unit may notify the executive body on its decision to recognize as suspicious, suspend, refuse or terminate a transaction or a business relationship, or to freeze the property of persons related to terrorism, provided that prior to issuing such

notification the report and the decision on recognizing as suspicious, suspending, refusing or terminating a transaction or a business relationship, or freezing the property of persons related to terrorism, have been submitted to the executive body.

2.10. The internal monitoring unit and customer service departments/employees of the Company shall work in constant collaboration, including the following:

2.10.1. The internal monitoring unit shall on a regular basis conduct training courses and seminars for customer service departments/employees of the Company, to introduce them to the updates in the field of money laundering and terrorism financing prevention, including the typologies;

2.10.2. The internal monitoring unit shall at all times provide the customer service departments/employees of the Company with the latest lists of non-cooperative countries and entities linked to terrorism published by the United Nations or the authorized body;

2.10.3. At the request of the internal monitoring unit the customer service departments/employees of the Company shall immediately make available to the unit any document or data related to customers, their transactions, and business relationships;

2.10.4. The customer service departments/employees must properly perform the duties assigned to them by points 7.7, 11.5, and 11.6 hereof.

3. Hiring, training, and retraining of the internal monitoring unit and other staff

3.1. The staff of the internal monitoring unit shall be hired pursuant to the procedure envisaged by the "Regulations of the Internal Audit Unit" and "Internal rules of work discipline" of the Company, while other staff responsible for preventing money laundering and terrorism financing, according to the procedure set out in the "Internal rules of work discipline".

3.2. In order to properly perform their duties under the Law, these Rules, and other legal acts adopted on the basis of the Law, staff members of the internal monitoring unit shall have higher education or a professional qualification certificate (in the field of finance) recognized in the Republic of Armenia or internationally. In the ten years preceding their appointment, they must also possess at least one year of work experience (in finance or in the field of combating money laundering and terrorism financing).

3.3. The staff member of the internal monitoring unit cannot be the a person, who:

3.3.1. Has a previous conviction for a premeditated crime;

3.3.2. Has been deprived by the court of the right to hold positions in financial, banking, tax and customs, commercial, economic or legal fields;

3.3.3. Has been recognized bankrupt and has unpaid (unwaived) liabilities;

3.3.4. Is involved in a criminal case by Armenian or foreign law enforcement agencies as suspect, accused, or defendant;

3.3.5. Does not meet the criteria specified in point 3.2 of these Rules.

3.4. The information stipulated by points 3.2 and 3.3 hereof shall be submitted through the Declaration on Staff Member of Internal Monitoring Unit (hereinafter: "the Declaration") approved by the authorized body, to be submitted to the Company before appointment as a staff member of the internal monitoring unit. Reliability of information contained in the declaration may be verified by any means not forbidden by the law.

3.5. The Company's staff related to the prevention of money laundering and terrorism financing shall have knowledge of the legislation on combating money laundering and terrorism financing, other legal acts (especially related to the responsibilities on performing customer due diligence and submitting reports on suspicious business relationship or transaction), as well as knowledge of current risks and typology associated with money laundering and terrorism financing.

3.6. To meet the requirement stipulated by point 3.5 hereof, the Company shall on a regular basis organize training on the prevention of money laundering and terrorism financing for the members of the Board, the executive body, internal monitoring unit, customer service, and internal audit department staff, as well as for other competent employees involved in money laundering and terrorism financing prevention activities. If new staff is employed, then the training on money laundering and terrorism financing prevention shall be held within the first three months following the start of their employment.

3.7. If new staff specified in point 3.6 is employed, then the training on money laundering and terrorism financing prevention shall be held within the first three months following the start of their employment.

3.8. Educational materials of the training arranged by the Company, as well as names of the attendees and documents verifying their participation in the training shall be recorded and kept for at least five years.

4. Risk management

4.1. Risk management is performed by the Company through the following two stages:

4.1.1. Risk assessment;

4.1.2. Taking measures to counter the risk.

4.2. The Company shall on a regular basis, but no less than annually, assess the existing and potential risks associated with money laundering and terrorism financing, as well as financing of the proliferation of weapons of mass destruction, and the measures it takes to mitigate them. Based on such assessment, the Company shall develop (review) its policy, procedures, and control mechanisms aimed at the effective management and mitigation of the identified risks.

4.3. Among other money laundering and terrorism financing related risks, the Company shall also identify and assess the existing and potential risks associated with the implementation of new services or methods for service provision, and the deployment of new or developing technologies, whereas the identification and assessment of the said risks shall be performed prior to the actual implementation of the new services or methods for service provision, or the deployment of new or developing technologies.

4.4. The assessment specified in point 4.2 shall encompass at least the following risk components:

4.4.1. Customer risk;

4.4.2. Service or financial instrument risk;

4.4.3. Financial channel risk;

4.4.4. Geographic risk.

4.5. The assessment specified in point 4.2. shall imply at least the following risk mitigation measures:

4.5.1. Transaction monitoring;

4.5.2. Proper customer identification;

4.5.3. Identification of politically exposed persons;

4.5.4. Transaction screening to identify matches with prohibited transactions;

4.5.5. Name screening to identify any matches with data containing negative implications;

4.5.6. Staff training;

4.5.7. Process management;

4.5.8. Submission of information to management.

4.6. The results of the activities defined in points 4.2 and 4.3 shall be documented and maintained pursuant to the procedure provided for in points 5.29-5.33 hereof.

4.7. The customer 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 shall be defined by the Law, these Rules, and other legal acts adopted on the basis of the Law.

4.8. The risk shall be assessed as medium (standard) whenever criteria of high or low risk are absent, except for the case stipulated under sub-point 4.10.2 of these Rules.

4.9. The risk shall be assessed as high whenever at least one criterion of high risk is present, except for the case stipulated under sub-point 4.10.3 of these Rules.

4.10. The risk shall be assessed as low whenever:

4.10.1. Only criteria of low risk are present;

4.10.2. A medium (standard) risk criterion is present, but the transaction in question is a low risk transaction stipulated under point 4.14 of these Rules;

4.10.3. A high risk criterion is present, but the transaction in question is a low risk transaction stipulated under point 4.14 of these Rules.

4.11. At the presence of several criteria pertinent to different risks, the risk shall be determined as per the higher risk criterion, except for the cases stipulated under sub-points 4.10.2 and 4.10.3 hereof.

4.12. Whenever a new criterion of risk is identified in the course of the business relationship with the customer, the Company shall revise the risk assessment of the customer and perform customer due diligence established for the newly determined risk.

4.13. The following shall be considered high risk criteria:

4.13.1. Legal persons or arrangements that are personal asset-holding vehicles;

4.13.2. Companies that have nominee shareholders or shares in bearer form;

4.13.3. Businesses and business relationships that are cash-intensive;

4.13.4. Companies that have unusual or excessively complex ownership structure;

4.13.5. Private banking activities;

4.13.6. Non-face-to-face business transactions or relationships;

4.13.7. 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;

4.13.8. Entities (including financial institutions) that are domiciled or reside in non-cooperative countries or territories, or come from such countries or territories;

4.13.9. Customers whose accounts are used to make frequent and inexplicable transfers to various financial institutions;

4.13.10. Customers whose transaction and/or business relationship structure or nature make it difficult to identify the real beneficiary;

4.13.11. Customers carrying out cash-based activities, including: customers providing cash services (e.g. cash transfer companies, exchange offices), casinos, entities organizing games of chance, or customers whose activities are not normally cash-based if using large amounts of cash for some of the transactions;

4.13.12. Not-for-profit entities;

4.13.13. Specialized entities carrying out accounting, legal, or similar activities that are serviced by financial institutions and act on behalf of their customers;

4.13.14. Intermediaries (financial and non-financial) whose activities are not regulated by the legislation on combating money laundering and terrorism financing;

4.13.15. Customers using bearer securities including bearer cheque books;

4.13.16. Any complicated or extraordinarily large transactions, as well as transactions or business relationships involving unusual conditions lacking obvious economic or other valid objectives.

4.14. The following shall be considered low risk criteria:

4.14.1. Payments to the state or community budgets of the Republic of Armenia;

4.14.2. Financial institutions that are effectively supervised in terms of money laundering and terrorism financing prevention;

4.14.3. Government bodies; local self-governance bodies; non-commercial organizations established by the state; state administrative institutions except for institutions or organizations located in non-cooperative countries or territories.

4.15. While applying the risk-based approach, the Company shall take the account of risk criteria which are typical of a specific customer or transaction and may affect the risk level to be determined thereon. Such criteria include:

4.15.1. Customer's business profile;

4.15.2. Customer's account objective or business relationship type;

4.15.3. Amount entered by the customer to their account or value of the transaction;

4.15.4. Regulatory, management, and supervision framework governing the financial institution;

4.15.5. The duration and structure of the business relationship;

4.15.6. Knowledge of the country, including understanding of the country's laws, regulations, and rules;

4.15.7. Involvement of intermediary legal entities or structures, which exist with no obvious economic objective or rationale, or unnecessarily complicate the transaction/business relationship and result in lack of transparency.

4.16. For risk management purposes, the Company shall perform the following:

4.16.1. Timely identify each customer and verify their identity;

4.16.2. Take steps to identify the real beneficiaries (beneficial owners), and, if any, identify them and verify their identity;

4.16.3. If a customer has an authorized representative, identify them and verify the authority to act on behalf of the customer;

4.16.4. Obtain information about the customer's financial standing and commercial activity including in order to obtain an understanding of the scope and the nature of anticipated transactions.

4.17. For the purpose of countering (managing) the potential and existing risks associated with the implementation of new types of services, or introduction of new ways to provide services using modern or developing technologies, the procedures to implement the said services must be discussed with the internal monitoring unit and must only be implemented upon receipt of approval from the latter.

4.18. To ensure effective risk management, when establishing a non-face-to-face business relationship or transaction, the Company shall:

4.18.1. Conclude agreements pursuant to the provisions of point 4 of the Company's regulation defining requirements to the internal monitoring system;

4.18.2. Make sure that the documents and orders required have been submitted by the customer through a designated mechanism using authorized electronic addresses, electronic signatures, or codes;

4.18.3. Within the framework of customer due diligence process, require that the payments be made through an account in the customer's name with a financial institution, which meets the requirements defined under sub-clauses "a" to "c" of Clause 3, Part 8 of Article 16 of the Law.

5. Customer due diligence (simplified and enhanced) and record keeping

5.1. Except for the case defined by point 5.35 of these Rules, the Company shall carry out customer 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 customer identification data (including documents);

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

5.2. The process of customer due diligence shall comprise identifying and verifying the identity of the customer (including that of the authorized person and the beneficial owner), understanding the purpose and intended nature of the transaction or business relationship, as well as conducting ongoing due diligence throughout the whole course of the business relationship (including the very moment of establishing a business relationship with a customer).

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

5.3.1. Obtain documents and information from the customer;

5.3.2. Review the documents and information obtained from the customer (if necessary, also from other sources) and determine the customer's business profile.

5.4. The first stage of customer due diligence shall be carried out by the Company's employees servicing the customer, while the second stage shall be performed by the internal monitoring unit.

5.5. Any business relationship with a customer may be established or an occasional transaction may be concluded by the Company only upon the receipt of the identification documents (information) specified in these Rules and upon verifying the customer's identity. The Company may verify the customer's identity based on the information required for identification in the course of establishing a business relationship or concluding an occasional transaction, or thereafter, within a reasonable timeframe, but no later than within seven days, if this is necessary for not disrupting the normal course of business relationship with the customer and provided that a managers of the Company or the servicing employee knows the customer personally and guarantees that all the required documents and information will be provided by the customer.

5.6. When identifying the customer, the Company shall also determine if the customer acts on their own or other person's behalf, and/or in their own or other person's interests, as well as shall:

5.6.1. Determine if an authorized person is appointed and if so, identify such authorized person pursuant to these Rules, check their identity and their authority to act on behalf of the customer;

5.6.2. Determine if a real beneficiary is present and if so, identify such real beneficiary pursuant to these Rules and check their identity.

5.7. If the customer is a legal entity, for the purpose of identifying the real beneficiary the Company shall obtain full information on the participants and the competence of the management bodies of the legal entity.

5.8. The Company shall identify the Customer and check their identity based on reliable and valid documents and other information provided by the state competent body and specialized competent institutions.

5.9. In order to identify an individual customer, their authorized person or real beneficiary, the Company shall request that the following documents be provided by the customer:

5.9.1. A copy of the identification document;

5.9.2. In case of private entrepreneurs, the number of the state registration certificate and a copy of the taxpayer (tax ID No.) registration or an equivalent document;

5.9.3. Statement on existence (absence) of a real beneficiary in the format defined by the authorized body;

5.9.4. Notice on residence / registration address if there is no indication of it in any of the other documents;

5.9.5. Document verifying the place of residence (utility or other service payment receipt, bank account note or statement, or any other document demonstrating that the customer resides at the mentioned address);

5.9.6. Statement on the centre of vital interests if the customer is a foreign entity and there is no indication of it in any of the other documents;

5.9.7. Any other document required under any internal regulation of the Company;

5.9.8. Any other document that the internal monitoring unit deems necessary to request.

5.10. In order to identify a customer that is a legal entity or its authorized person, the Company shall request that the following documents be provided by the customer:

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

5.10.2. Copy of the taxpayer (tax ID No.) registration or an equivalent document;

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

5.10.4. List of individuals who are authorized to represent the customer without a power of attorney and copies of documents verifying their appointment;

5.10.5. List of individuals who are authorized to represent the customer based on a power of attorney, as well as documents verifying their authorities or copies thereof;

5.10.6. Statement on existence (absence) of a real beneficiary in the format defined by the authorized body;

5.10.7. For persons specified in sub-points 5.10.4-5.10.6 hereof, documents stipulated by point 5.9 except for sub-point 5.9.3;

5.10.8. List of persons who own twenty percent or more of the customer's equity securities;

5.10.9. Statement on the centre of vital interests if the customer is a foreign entity and there is no indication of it in any of the other documents;

5.10.10. Any other document required under any internal regulation of the Company;

5.10.11. Any other document that the internal monitoring unit deems necessary to request.

5.11. In order to identify a customer that is a state or local government authority or its authorized person, the Company shall request that the following documents be provided by the customer:

5.11.1. Statement showing the full name and the country of the state or local government authority;

5.11.2. Any other document required under any internal regulation of the Company;

5.11.3. Any other document that the internal monitoring unit deems necessary to request.

5.12. Based on the documents specified in points 5.9-5.11 hereof, the internal monitoring unit shall perform the risk assessment for the customer and the concluded transaction or business relationship, based on which a decision is made whether simplified, enhanced, or standard procedure will apply to further customer due diligence.

5.13. In case of medium (standard) risk, the process of customer due diligence as defined under Clause 19, Part 1 of Article 3 of the Law shall be applied, whereby the Company, in implementation of the requirements established under that Clause and other relevant provisions of the Law for medium (standard) risk, shall take regular measures for ongoing due diligence of the business relationship.

5.14. When performing scrutiny of transactions within the framework of ongoing due diligence of the business relationship, the Company shall take the following regular measures in case of medium (standard) risk:

5.14.1. Ascertain veracity and reliability of information (including documents) requested from the customer in relation to the transactions or the business relationship, by means of, inter alia, searching limited access and publicly available sources of information, making inquiries to competent authorities and other reporting entities, as well as foreign counterparts, as necessary;

5.14.2. Collate sources, movements and volumes of the funds circulated through different transactions within the reviewed period of time;

5.14.3. Check the existence of links between customers, transactions and business relationships;

5.14.4. Ascertain consistency of the transactions or the business relationship with the business profile of the customer;

5.14.5. If there are suspicions about the legitimacy of the customer's revenues or wealth, establish the sources thereof.

5.15. In case of high risk, the process of enhanced customer due diligence as defined under Clause 22, Part 1 of Article 3 of the Law shall be applied, whereby the Company, in implementation of the requirements established under that Clause and other relevant provisions of the Law for high risk, shall take advanced measures for ongoing due diligence of the business relationship.

5.16. When performing scrutiny of transactions within the framework of ongoing due diligence of the business relationship, the Company shall take the following advanced measures in case of high risk:

5.16.1. Request necessary information (including additional documents), search all limited access and publicly available sources of information, make inquiries to as many as possible competent authorities and other reporting entities, as well as foreign counterparts, when ascertaining veracity and reliability of information (including documents) requested from the customer in relation to the transactions or the business relationship;

5.16.2. Take an as longer as possible or several comparable reviewed periods of time, when collating sources, movements and volumes of the funds circulated through different transactions;

5.16.3. Conduct a multi-level analysis, including one for discovering indirect links, when checking the existence of links between customers, transactions and business relationships;

5.16.4. Request information (including documents) fully substantiating the actions taken within the framework of the transactions or the business relationship, when ascertaining their consistency with the business profile of the customer;

5.16.5. Request information (including documents) substantiating the legitimacy of the funds and wealth of the customer, when establishing their source.

5.17. In case of low risk, the process of simplified customer due diligence as defined under Clause 24, Part 1 of Article 3 of the Law may be applied, whereby the Company, in implementation of the requirements established under that Clause and other relevant provisions of the Law for low risk, may take lightened measures for ongoing due diligence of the business relationship.

5.18. When performing scrutiny of transactions within the framework of ongoing due diligence of the business relationship, the Company may take the following lightened measures in case of low risk:

5.18.1. Ascertain veracity and reliability of information (including documents) requested from the customer in relation to the transactions or the business relationship based on the information submitted by the customer;

5.18.2. Collate sources, movements and volumes of the funds circulated through different transactions within the reviewed period of time only when they exceed a reasonable monetary threshold;

5.18.3. Check the existence of links between customers, transactions and business relationships only when links with medium (standard) or high risk customers, transactions or business relationships emerge.

5.19. Scrutiny of transactions within the framework of ongoing due diligence of the business relationship shall be performed throughout the course of the business relationship (including the very moment of establishing a business relationship with a customer); at that, the measures stipulated under sub-points 5.14.2, 5.14.3, 5.16.2, and 5.16.3 hereof shall be taken no later than:

5.19.1. Once a year – in case of medium (standard) risk;

5.19.2. Once in six months – in case of high risk (except for the case stipulated under sub-point 5.23 hereof.

5.20. Updating of the data collected within the framework of customer due diligence (except for the data obtained through identification and verification of identity of customers) shall be performed no later than:

5.20.1. Once a year – in case of medium (standard) risk;

5.20.2. Once in six months – in case of high risk (except for the case stipulated under sub-point 5.23 hereof);

5.20.3. Once in two years – in case of low risk.

5.21. Updating of the data collected during the identification and verification of identity of customers shall be performed once a year.

5.22. Customer due diligence measures shall be applied to the existing customers, as at the date of bringing in the new requirements of national legislation, by taking measures commensurate to the risk of money laundering and terrorism financing, in the following cases and timeframes:

5.22.1. In relation to identifying and verifying the identity of the customer (including that of the authorized person and the beneficial owner), as well as understanding the purpose and intended nature of the transaction or business relationship – before conducting the first transaction with the customer or updating the data collected within the framework of customer due diligence as stipulated under point 5.21 hereof, whichever occurs earlier after the enactment of the new requirements;

5.22.2. In relation to conducting ongoing due diligence of the business relationship – upon enactment of the new requirements.

5.23. In case of politically exposed persons, the enhanced ongoing monitoring defined under Sub-Clause “d”, Clause 22, Part 1 of Article 3 of the Law shall comprise the measures specified

under point 5.16 hereof, which, except for the cases stipulated under points 5.19 and 5.20 hereof, shall be taken no later than once in three months.

5.24. The declaration of existence (absence) of a beneficial owner in the course of the business relationship shall be filled in by the Customer also whenever a beneficial owner appears, or whenever the beneficial owner is changed.

5.25. In performing the enhanced ongoing monitoring defined under Sub-Clauses “a” and “b”, Clause 19, Part 1 of Article 3 of the Law the Company may use information obtained by other financial or non-financial institutions or entities as a result of the customer due diligence, provided that:

5.25.1. Such information is obtained by the Company directly from the other financial or non-financial institution or entity;

5.25.2. The Company takes necessary steps to make sure that the other financial or non-financial institution or entity is:

5.25.2.1. Entitled and able to immediately upon request provide information obtained as a result of the customer due diligence, including copies of documents;

5.25.2.2. Subject to proper regulation and supervision in the field of money laundering and terrorism financing prevention, as well as have effective procedures in place for customer due diligence and information maintenance pursuant to the provisions of the Law and legal acts adopted based thereon;

5.25.2.3. Not domiciled or residing in, or coming from, a non-cooperative country or territory.

5.26. Documents and information received from the Customer as part of the customer due diligence process may be in Armenia, Russian, or English. Documents submitted in any other language than these shall have a translation into Armenian verified by notary public.

5.27. Documents presented by foreign entities in languages other than Armenian shall be submitted with apostille or consular legalization, unless the Company’s consent has been obtained on submitting them without the latters.

5.28. In case of correspondent or other similar relationship with foreign financial institutions, the Company, in addition to the customer due diligence requirements stipulated by the Law and these Rules, shall:

5.28.1. Gather sufficient information so as to understand fully the nature of foreign financial institution’s business and, from publicly available and other reliable information, to determine the business reputation of the institution and the quality of its supervision, including whether it has been subject to a money laundering or terrorism financing criminal investigation or any other proceeding;

5.28.2. Assess the foreign financial institution’s internal procedures for combating money laundering and terrorism financing to make sure that they are adequate and effective;

5.28.3. Obtain approval from senior management before establishing new correspondent or other similar relationships;

5.28.4. Document the duties of each foreign financial institution with regard to combating money laundering and terrorism financing if they are not expressly set out;

5.28.5. In case of transit account make sure that the foreign financial institution:

5.28.5.1. Has conducted due diligence of customers having direct access to the accounts of the financial institution and is able to provide upon request relevant data regarding the due diligence of these customers

5.28.5.2. Does not allow the use of its accounts by shell banks.

5.29. The Company should maintain the information (including documents) required under these Rules and the Law, including the information (documents) obtained in the course of customer due diligence, regardless of the fact whether the transaction or business relationship is ongoing or has been terminated, inclusively of:

5.29.1. Customer identification data, including the data on the account number and turnover, as well as business correspondence data;

5.29.2. All necessary records on transactions or business relationships, both domestic and international (including the name, the registration address (if available) and the place of residence (domicile) of the customer (and the other party to the transaction), the nature, date, amount, and currency of transaction and, if available, type and number of the account), which would be sufficient to permit full reconstruction of standalone transactions or business relationships;

5.29.3. Information on suspicious transactions or business relationships as specified under Article 7 of the Law, as well as information concerning the process of review (conducted analysis) and findings on transactions or business relationships not recognized as suspicious;

5.29.4. Findings of the assessment of potential and existing money laundering and terrorism financing risks specified under points 4.2, 4.3 hereof;

5.29.5. Other information specified under these Rules and the Law.

5.30. Information (including documents) specified under point 5.29 of these Rules should be maintained for at least five years following the termination of the business relationship or completion of the transaction, or for a longer period if required by the law.

5.31. Information (including documents) required under the Law and these Rules and maintained by the Company should be sufficient to enable submission of comprehensive and complete data on customers, transactions, or business relationships whenever requested by the authorized body or, in cases established by the law, by criminal prosecution authorities.

5.32. Information (including documents) established by these Rules and the Law can be collected and maintained in paper or electronic form.

5.33. Information (including documents), which these Rules and the Law require to maintain, should be recorded. Recording should be done in a way enabling reconstruction of identity

of the employee, who had performed customer due diligence or had taken other actions for obtaining information (including documents) to be maintained.

5.34. Customer due diligence procedure established by these Rules shall not be applied to transactions carried out by the Company for its own needs as part of the normal course of business (except for buying financial assets).

5.35. If within the deadline established by the Company the customer does not submit to the Company the information required to take actions established under points 5.20, 5.21 of these Rules, then the Company shall have the right to suspend service provision to the customer until such time that the documents are provided.

6. Collecting, recording, and maintaining of information on transactions and business relationships

6.1. Collecting and recording information on transactions and business relationships shall be implemented by the employees immediately involved in customer service or immediately conducting the transactions, and where necessary by the staff of internal monitoring unit.

6.2. Collecting information on transactions and business relationships may be implemented in documentary or electronic form.

6.3. Information on transactions and business relationships shall be recorded in databases managed by, or at all times accessible to, the Company.

6.4. Maintaining of information on transactions and business relationships shall be governed by the requirements of points 5.30-5.33 of these Rules.

7. Recognizing a transaction or a business relationship as suspicious

7.1. The Company must recognize a transaction or business relationship, including an attempted transaction or business relationship, as suspicious and file with the authorized body a report on suspicious transaction or business relationship as stipulated under Article 8 of the Law, if it is suspected or there are reasonable grounds to suspect that the property involved 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 must consider recognizing a transaction or business relationship as suspicious and filing with the authorized body a report on suspicious transaction or business relationship 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 clear for the Company that, although there is no suspicion arising from a specific criterion or typology of a suspicious transaction or business relationship, the logic, pattern (dynamics) of implementation or other characteristics of the performed or attempted transaction or business relationship provide 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 filing with the authorized body a report on suspicious transaction or business relationship as stipulated under Article 8 of the Law, the grounds for non-recognition of the transaction or business relationship as suspicious, the respective conclusions, the process of conducted analysis and its findings shall be documented and maintained 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 of the Company 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 shall commence both upon receiving internal or external signals, as well as upon the initiative of the internal monitoring unit, whenever:

7.5.1. There is a potential match of the data on a customer or on the other party to a transaction with the identification data of the persons related to 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 performed or attempted transaction or business relationship provide 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 customer service staff, the management bodies of the Company, the internal audit, as well as from other staff with competencies in the prevention of money laundering and terrorist financing. Such signals shall be transmitted to the internal monitoring unit in the manner and timeframes established by internal regulations.

7.7. Internal signals should 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, other reporting entities, foreign counterparts, as well as from limited access and publicly available sources of information.

7.10. In cases specified under sub-point 7.5.1 of these Rules, the internal monitoring unit shall take the following measures, whenever there is a potential match of the data with:

7.10.1. Identification data of the persons related to 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, file with the authorized body a report on suspicious transaction or business relationship 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 to 7.5.3 of these Rules, the internal monitoring unit shall within reasonable time conduct comprehensive analyses by using customer 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, file with the authorized body a report on suspicious transaction or business relationship 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 transaction or business relationship for a period of up to five days and immediately file a report with 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 be obligated to suspend the transaction or business relationship for five days and immediately file a report with 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 should 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, containing mandatory specification of the period of suspension of suspicious transaction or business relationship. The internal monitoring unit shall notify the executive body of the Company on this 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 customer record file.

8.6. If within five days upon sending of the notice on suspending a transaction or business relationship by the Company to the authorized body, or upon the suspension of a transaction or business relationship by the authorized body, no notice on extending the suspension or repealing the decision on suspension is communicated by the authorized body to the Company, the decision on suspension shall be considered as repealed, the suspension shall be terminated, and a relevant note to this effect is made in the customer record file.

8.7. The decision of the Company or the authorized body on suspending a transaction or business relationship may be repealed 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 is determined that the suspicion of money laundering or terrorism financing is groundless, the CEO of the Company based on the proposal of the internal monitoring unit of the Company submits to the authorized body a request on repealing transaction or business relationship suspension before the end of the suspension period.

8.9. On the basis of the decision of the authorized body on repealing the suspension before the end of the suspension period made on the basis of either the request specified in point 8.8 or the initiative of the authorized body, the internal monitoring unit makes a decision on repealing 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 customer record file.

9. Refusal or termination of a suspicious transaction or business relationship

9.1. Where the customer due diligence related requirements defined under the Law and these Rules cannot be implemented, the Company should refuse the transaction or business relationship and consider recognizing it as suspicious.

9.2. The Company must refuse the transaction or business relationship and consider recognizing it as suspicious also where an assignment has been received on refusing a transaction or business relationship as specified under Clause 6, Part 1 of Article 10 of the Law.

9.3. The internal monitoring unit adopts a written decision on refusal of the transaction or business relationship in the case specified in point 9.1 of these Rules. The internal monitoring unit shall notify the executive body of the Company on this decision.

9.4. 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, and notify the customer accordingly.

10. Freezing of assets belonging to entities linked to terrorism

10.1. The assets owned or controlled directly or indirectly by terrorism-related 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 shall be subject to freezing by the Company without delay and without prior notice to the persons involved.

10.2. The assets of a customer 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 assets of a customer. The internal monitoring unit shall notify the executive body of the Company on this decision.

10.4. Information about customer, its assets and freezing thereof based on the decision of the internal monitoring unit or the authorized body shall be registered in the customer's record file.

10.5. Upon freezing of the assets of the terrorism-related person the Company shall without delay proceed to recognize the transaction or business relationship as suspicious, and to file a report on suspicious transaction or business relationship.

10.6. The assets of bona fide third parties, i.e. the persons who, when passing the assets 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 assets, 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 freezing shall be revoked only by the authorized body, if the assets have been frozen by mistake, as well as when the criminal prosecution body arrests the frozen assets. The freezing of the assets of the persons specified under Part 2 of Article 28 of the Law shall also be revoked whenever it is established that the person with frozen assets has been removed from the list of terrorism-related persons.

10.8. Information about the revocation of the freezing shall be registered in the customer's record file.

11. Submission of reports to the authorized body

11.1. The Company shall file reports with the authorized body on suspicious transactions or business relationships and (or) on transactions subject to mandatory reporting.

11.2. Reports or suspicious transactions or business relationships shall be filed by the Company, regardless of the amounts involved.

11.3. Unless otherwise established by the authorized body, mandatory transaction reports shall be filed for the following transactions:

11.3.1. Non-cash transactions with value equal to or exceeding AMD 20 million;

11.3.2. Cash-involving transactions with value equal to or exceeding AMD 5 million.

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

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

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

11.7. In the case specified under point 11.6 hereof the internal monitoring unit within three business days upon receipt of the information shall compile a report on the transaction in the manner and form required by the authorized body and file it with the latter.

11.8. In the case specified under point 11.5 hereof 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 7 of these Rules.

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

12. Prohibited Activities

12.1. In addition to the prohibition to carry out transactions with entities linked with terrorists and terrorism, the following activities will also be prohibited within the Company:

12.1.1. Open anonymous accounts or accounts in fake names;

12.1.2. Open accounts marked by digits, letters, or other symbols only;

12.1.3. Perform transactions with bearer securities;

12.1.4. Provide services to, or carry out transactions with, non-licensed banks and non-bank financial institutions (except if no licensing is required by the legislation);

12.1.5. Provide services to, or carry out transactions with, shell banks;

12.1.6. Deal, in any way, with any institutions that provide services to shell banks;

12.1.7. Provide services to, or otherwise deal with, money transfer agents or organizations offering similar services whose activities are unlicensed or unregulated.

13. Audit

13.1. The Company shall conduct internal audit to ascertain that its activities comply with the requirements of the Law, these Rules and other legal acts based on the Law.

13.2. At least once a year, the CEO of the Company shall appoint an auditor or form an audit group, which conducts a review to ascertain that the executive body and the internal monitoring unit ensure the full compliance of the Company with the requirements established by the Law, these Rules and other legal acts based on the Law.

13.3. The group specified in point 12.2 hereof shall comprise at least two members who shall be employees of the Company, however, must not be members of the executive body or the internal monitoring unit, or a person immediately involved in performing customer identification and due diligence pursuant to these Rules.

13.4. Based on the implementation of the requirements defined under point 12.2 hereof, the auditor or the audit group shall compile a report, which shall be submitted to the executive body for approval.

13.5. Within one week upon approval by the executive body of the Company, the report compiled as a result of the implementation of the requirements defined under point 12.2 hereof shall be duly submitted to the authorized body.

13.6. During the course of the annual independent audit of the Company's financial and economic activities, the independent audit firm shall among other things review the implementation in the Company of the provisions of the legislation on combating money laundering and terrorism financing, and the effectiveness of complying therewith.

13.7. Within a month upon receipt from the authorized body of a request to have an independent audit performed, the Company shall contract an independent audit firm. Within a week upon receipt of the independent audit report, it shall be submitted to the authorized body.