Approved by the resolution N Ո-25-001 of sole partcipant
of "Aktina Capital" limited liability company
Director: Tigran Davtyan

May 12, 2025

AKTINA CAPITAL LIMITED LIABILITY COMPANY

"PROCEDURE ON COMPLIANCE WITH ANTI-MONEY LAUNDERING, COUNTER-TERRORISM FINANCING, AND INTERNATIONAL SANCTIONS"

Yerevan
2025

CONTENT

PURPOSE

Procedure on Combating Money Laundering, Terrorist Financing, and Compliance with International Sanctions (hereinafter referred to as the "**Procedure**") aims to ensure the compliance of **Aktina Capital LLC** (hereinafter referred to as the "**Company**"), an investment company, with measures to prevent money laundering and terrorist financing (hereinafter "**ML/TF**"), adherence to international sanctions, as well as the prevention of financing the proliferation of weapons of mass destruction (hereinafter "**WMD Financing**").

This Procedure defines the key functions, principles, requirements, and implementation framework of the Company's internal controls for combating ML/TF/WMD Financing. It also regulates relationships related to the freezing of assets of persons involved in terrorist financing.:

SCOPE OF APPLICATION

The provisions of this Procedure apply to all governing bodies, executives, structural and territorial units (hereinafter referred to as "**Units**"), and employees of the Company.

RELATED DOCUMENTS

1. "Policy on Combating Money Laundering, Terrorist Financing and Compliance with International Sanctions".
2. "Law of the Republic of Armenia on Combating Money Laundering and Terrorist Financing"
3. "Regulation on Minimum Requirements for Persons Reporting in the Field of Anti-Money Laundering and Counter-Terrorist Financing" (Approved by Decision No. 279-N of the Board of the Central Bank of Armenia dated 07.10.2014)
4. "Guideline on Indicators of High Risk and Suspicion Related to Money Laundering and Terrorist Financing" (Approved by Decision No. 1/711-A of the Chairman of the Central Bank of Armenia dated October 11, 2016)
5. "Procedure for Completion and Submission of Report Form No. 106 on Transactions and Suspicious Transactions or Business Relationships Subject to Mandatory Reporting by Persons Providing Investment Services, Corporate Investment Funds, and Non-Public Contractual Investment Funds without Licensed Managers under the Law on Securities Market of the Republic of Armenia"

ANNEXES

1. **Annex 1** – List of Required Documents for Establishing Business Relationship (Individual)
2. **Annex 2** – *List of Required Documents for Establishing Business Relationship (Legal Entity)*
3. **Annex 3** – *List of Required Documents for Establishing Business Relationship (Financial Institution)*
4. **Annex 4** – *"Know Your Customer" (KYC) Questionnaire (Individual)*
5. **Annex 5** – *"Know Your Customer" (KYC) Questionnaire (Legal Entity and Sole Proprietor)*
6. **Annex 6** – *"Know Your Customer" (KYC) Questionnaire (Financial Institution)*

7. **Annex 7** – *Table of High-Risk Indicators*
8. **Annex 8** – *Suspicious Transaction Reporting Form (for Employees)*
9. **Annex 9** – *Training Form on AML/CFT and Sanctions Compliance*

DEFINITIONS[1]

1. **Know Your Customer (KYC) Principle** – An internationally accepted principle requiring the identification and collection of personal data of a Customer, clarification of the Customer's business profile, periodic updating of the gathered information, and application of due diligence measures to the Customer and their transactions.
2. **Company's Screening Software** – A licensed database solution used by the Company that includes UN, EU, OFAC, OFSI, and PEP lists, as well as adverse media or other negative signals and information related to individuals or companies.
3. **Company's Governing Bodies** – Includes the Chief Executive Officer and the General Meeting of Participants of the Company.
4. **Front-Line Employees** – Employees involved in customer service, client interactions, business operations, and post-operational departments of the Company.
5. **Customer Identification Data Folder** – A centralized internal storage system containing individually labeled electronic folders for each Customer. These folders include documents submitted by the Customer and/or related to the Customer, contracts, results of screening procedures, audio-visual materials (photos and videos), and other supporting evidence.

CHAPTER 1. GENERAL PROVISIONS

1.1. This Procedure is developed in accordance with the provisions of the Law of the Republic of Armenia "On Combating Money Laundering and Terrorist Financing" (hereinafter referred to as the "Law"), the normative legal acts of the Central Bank of Armenia (CBA) adopted based on the Law, the FATF standards, international best practices, and the requirements of the Company's internal AML/CTF Policy.

1.2. The heads of the respective structural units of the Company are responsible for organizing and ensuring the implementation of the specific functions/steps forming part of the processes defined in this Procedure within their respective departments.

1.3. The Company's anti-money laundering and counter-terrorist financing (AML/CTF) system is aimed at preventing money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction (ML/TF/FPWMD), as well as establishing effective mechanisms for responding to international sanctions.

---

[1]All terms used in this Procedure shall have the meanings ascribed to them in the Company's "Anti-Money Laundering, Counter-Terrorist Financing, and International Sanctions Compliance Policy" (hereinafter referred to as the "Policy") and the Law of the Republic of Armenia "On Combating Money Laundering and Terrorist Financing".

CHAPTER 2. MINIMUM RULES FOR ESTABLISHING A BUSINESS RELATIONSHIP AND CONDUCTING CUSTOMER DUE DILIGENCE

2.1. The Company shall perform customer due diligence (CDD) in the following cases:
- 2.1.1. when establishing a business relationship;
- 2.1.2. when there are doubts as to the veracity or adequacy of the information (including documents) previously obtained for the purposes of customer identification;
- 2.1.3. when there are suspicions of money laundering or terrorist financing.

2.2. The CDD process includes the identification and verification of the Customer (including the authorized person and beneficial owner), as well as determining the purpose and intended nature of the transaction or business relationship.

2.3. The following are subject to customer due diligence:
- 2.3.1. All Customers of the Company, regardless of the type of business relationship established with them;
- 2.3.2. Shareholders and/or beneficial owners, and executives (managers) of legal entities;
- 2.3.3. Authorized persons;
- 2.3.4. Individuals with signatory rights without power of attorney;
- 2.3.5. The Company's suppliers and agents;
- 2.3.6. The Company's counteragents.

2.4. Customer identification at the Company is performed either in person or remotely via audiovisual telecommunication means, including an online video recording platform, following the document verification stage based on documents provided in advance by the Customer. To ensure implementation of identification and compliance with KYC requirements, the responsible employee of the servicing unit shall, at a minimum, take the following steps:
- 2.4.1. Send the list of required documents defined in the annexes to this Procedure (Annexes 1, 2, 3) to the Customer, and provide the “Know Your Customer” (KYC) questionnaire to be completed by the Customer;
- 2.4.2. Collect all documents listed in the prescribed list, verify the validity periods and their compliance with the required list, and ensure that the KYC questionnaire is properly completed and signed.

2.5. Following the collection of the documents referred to in Clause 2.4 of this Procedure and receipt of the signed “Know Your Customer” (KYC) questionnaire, the responsible employee of the servicing unit shall perform a verification of the submitted documents and reconcile the data.

2.6. In case of incomplete or insufficient documentation, where it is not possible to identify the Customer, the responsible employee of the servicing unit may refrain from conducting due diligence and may suspend the process of establishing a business relationship until all required information and documents have been duly provided.

2.7. Once the document package is complete, the responsible employee of the servicing unit shall forward it through the Company’s internal communication system to the Compliance Officer (CO) for further verification and issuance of an opinion regarding the establishment of the business relationship.

2.8. In parallel with verifying the authenticity of documents and the consistency of the Customer's business profile with the submitted data, the CO shall also conduct a name screening of the Customer against restricted access databases, including UN, EU, OFAC, lists of Politically Exposed Persons (PEPs), as well as internal or authorized body-provided watchlists. In the absence of matches or adverse information, the process of establishing the business relationship with the Customer shall proceed.

2.9. If a match is found in any of the aforementioned lists, the establishment of the business relationship/transaction with the Customer requires the CO’s approval. The CO may request additional documents or information if the initially submitted documents do not allow for confirmation or elimination of the match. Such documents may include, but are not limited to, extracts from the Customer’s employment record, a certificate of no criminal record, a reference

letter from a reputable financial institution, or other documents as may be appropriate to the specific case.

2.10. The Customer identification process via audiovisual telecommunication means consists of an online video call, during which the responsible employee of the servicing unit communicates with the Customer through a Q&A session to verify the authenticity of the information provided in the KYC questionnaire. The employee conducts remote identification and ensures that the video recording is stored in the Customer's electronic file folder.

2.11. During the video call with an individual Customer, the responsible employee of the servicing unit shall:

2.11.1. establish a video connection with the Customer through the online platform,

2.11.2. verify the Customer's liveness and the authenticity of the identification data, including requesting the Customer to state their full name, date of birth, and compare the information with the data provided in the "Know Your Customer" (KYC) questionnaire,

2.11.3. request the Customer to reconfirm their intention to establish a business relationship and/or carry out a transaction,

2.11.4. request the Customer to present their identification document in a way that both the document and the Customer's facial features are clearly visible and can be photographed simultaneously,

2.11.5. upon request of the Compliance Officer (CO), discuss and record any outstanding issues identified during the due diligence process and, if necessary, make amendments to the KYC questionnaire.

2.12. During the video call with a legal entity Customer, the responsible employee of the servicing unit shall:

2.12.1. establish a video connection with the Chief Executive Officer (Director) of the legal entity Customer via the online platform,

2.12.2. verify the authenticity of the legal entity's identification data and compare it with the information provided in the KYC questionnaire,

2.12.3. request the Director to reconfirm the intention to establish a business relationship and/or carry out a transaction,

2.12.4. request the Director to present their identification document in such a way that both the document and the facial features of the individual are clearly visible and can be photographed simultaneously,

2.12.5. upon request of the CO, discuss and record any outstanding issues identified during the due diligence process (if any), and if necessary, amend the KYC questionnaire.

2.13. During the due diligence process of supervised financial institutions, no video call is conducted with the executive body of the respective institution, based on the oversight in place over such institutions, except in cases where the Compliance Officer (CO) has doubts regarding the authenticity of information obtained during the due diligence process.

2.14. If the identification documents of a legal entity Customer submitted under the procedure defined in Clause 2.4 of this Procedure are notarized or apostilled, and the responsible employee of the servicing unit is confident in their validity, the executive body of the legal entity may not be required to present additional identification documents.

2.15. The entire video call process is recorded, and the video recording must be stored in accordance with the procedure and timeframe defined by law, in the Company's internal network, in a dedicated folder created for each Customer.

2.16. When establishing a business relationship with a legal entity, the responsible employee of the servicing unit shall obtain complete information regarding the entity's participants, governing bodies, and their respective powers, in order to identify the beneficial owner.

2.17. As a result of the above process, the Customer is assigned a money laundering and terrorism financing (ML/TF) risk level—low, medium, or high. This risk level is recorded in the Company's software system and may only be changed by the CO upon instruction delivered

through the Company's internal communication system.

2.18. The information provided allows the CO to assess the Customer's risk and later to determine whether the transactions carried out align with the Customer's business profile, or if they are suspicious or potentially unlawful.

2.19. CO approval is also required in all cases where the Customer has high-risk indicators. High-risk indicators are defined in Appendix 7 to this Procedure and the CBA Guidelines on High-Risk and Suspicious ML/TF Indicators, but are not limited to them.

2.20. When establishing a business relationship with a high-risk Customer, the CO conducts enhanced due diligence and may request additional information or documents prior to executing the transaction or opening the account, if deemed necessary based on professional judgment. For Customers with low or medium risk, the standard servicing procedure applies.

2.21. Based on the collected data, the CO conducts an analysis comparing the Customer's business profile with the nature of the intended transactions using matching methodologies and data obtained from publicly accessible and specialized paid databases, then performs an assessment and makes a final decision regarding the establishment of a business relationship with high-risk Customers.

2.22. If the CO has been provided with all necessary information, an opinion on the approval or rejection of the business relationship is issued within a maximum of 3 business days. Otherwise, this timeframe starts from the date the final required document is received.

2.23. If the Customer refuses to provide the required identification documents or the requested information in the "Know Your Customer" questionnaire regarding their business profile, or provides false or incomplete information, the establishment of a business relationship with that Customer shall be denied.

2.24. If, during the due diligence process, it is revealed that there is another beneficial owner and it is not possible to identify and verify the identity of that person, the Company shall not execute the transaction and/or shall terminate the business relationship.

2.25. All information related to rejected business relationships/transactions, including the reasons for rejection, shall be recorded and maintained by the Compliance Officer (CO) in accordance with the procedures and timeframes defined by law.

2.26. If the establishment of a business relationship with a Customer is rejected by frontline employees, the data of the rejected Customer must be submitted to the CO for registration and inclusion in the Company's internal watchlists. This provision also applies to existing Customers when data updates are required and the Customer refuses to provide such information.

2.27. If, during the process of establishing a business relationship or servicing a Customer, any employee of the Company becomes aware of or has reason to suspect that the Customer has been rejected by another local or foreign financial institution, they must inform the CO in writing, including the information and possible grounds, for the purpose of conducting additional due diligence.

2.28. A frontline employee may refrain from conducting full Customer due diligence, except for identification and identity verification, only if there are suspicions of money laundering or terrorist financing and they reasonably believe that conducting the full due diligence would alert the Customer to such suspicions. In this case, the employee must immediately inform the CO via email.

2.29. The CO conducts a semi-annual review of Customer data, the completeness of such data in the Company's software system, and a sample-based review of the "Know Your Customer" questionnaires to monitor the quality of data entries. Identified deficiencies are documented and discussed with the head of the responsible department, and advisory support is provided to prevent similar issues in the future. In the case of material discrepancies, the CO includes them in the report submitted to the Company's Executive Body/Management and the meeting of shareholders or participants.

2.30. For the purposes of due diligence, the documents and information received from the Customer

may be submitted in Armenian, Russian, or English. Documents submitted in other languages must be translated into Armenian or one of the aforementioned languages with a notarized translation.

2.31. Documents submitted by foreign persons in a language other than Armenian must be apostilled or consularly legalized, unless the Company has agreed to accept such documents without an apostille or consular legalization.

CHAPTER 3: CASES WHERE BUSINESS RELATIONSHIPS WITH CUSTOMERS SHALL NOT BE ESTABLISHED

3.1. The Company shall not establish a business relationship with persons who fall outside the Company's risk appetite as defined in Annex 7 to this Procedure and in the Policy, as well as in the following cases:

- 3.1.1. With individuals or legal entities, and their family members, who are included in blacklists or are subject to international comprehensive sanctions,
- 3.1.2. Shall not conclude transactions involving securities issued by persons included in sanction lists,
- 3.1.3. With persons located, residing, or operating in non-compliant countries or territories,
- 3.1.4. With specialized intermediaries, trust organizations, and fiduciary accounts where the beneficial owner is not identified and/or enhanced due diligence is not possible,
- 3.1.5. Where there are suspicions regarding the sources of funds and income and/or enhanced due diligence cannot be performed,
- 3.1.6. When it is apparent that the Customer is being directed by another third party,
- 3.1.7. With persons engaged in the provision of services or production, delivery, sale, or resale of goods that have dual-use or potentially dangerous and negative environmental or social impact, such as the production, delivery, or sale of narcotics and arms/weapons,
- 3.1.8. With unlicensed payment and settlement organizations,
- 3.1.9. With persons or companies engaged in the sale, exchange, or cash-out of cryptocurrencies,
- 3.1.10. The Company shall not open anonymous or fictitious accounts, nor accounts represented solely by numeric, alphabetic, or symbolic designations,
- 3.1.11. The Company shall not service bearer securities or establish any type of business relationship with shell banks or with financial institutions that service shell banks.

3.2. All employees of the Company bear responsibility for the proper execution of the obligation not to establish business relationships with the above-mentioned types of Customers. In order to identify such cases, the CO carries out regular monitoring. If such cases are discovered, the Company terminates the business relationship with the respective Customers upon the CO's request.

3.3. In addition to the above-mentioned sectors, if an employee encounters any suspicious or unclear situation, they must consult with the CO to obtain an opinion on whether to establish or refuse the business relationship or carry out the transaction.

CHAPTER 4: RISK CLASSIFICATION

4.1. To assess the risks of customers and transactions, the Company follows a risk-based approach to prevent and detect potential suspicious transactions and business relationships, and to manage them effectively.

4.2. This approach is based on classifying Customers according to their risk level. In order to assess the Customer's/transaction's risk, three factors are considered: country or geographical risk,

customer, transaction or business relationship risk, product, service or delivery method risk. Following the assessment, the risk is categorized as Low, Medium (Standard), or High.

4.3. If several risk criteria are present simultaneously, the risk level shall be determined according to the highest risk criterion, except in cases defined by the regulation on the implementation of minimum AML/CFT requirements of the Republic of Armenia.

4.4. The Customer's risk level is determined through a model developed by the CO (see Annex 7), considering high-risk indicators. During the process of establishing a business relationship, front-line staff classify Customers and assign them a risk level based on the criteria defined in Annex 7. If no high-risk indicators under Annex 7 are present but there is a reasonable suspicion, front-line staff shall refer the case to the CO for determination of the Customer's risk level.

4.5. The risk level assigned by the front-line staff is entered into the Company's software system, which is monitored by their supervisor and the CO during ongoing Customer data monitoring.

4.6. The risk classification of a Customer may be revised either by front-line staff after updating the Customer's data or by the initiative of the CO when high-risk indicators are identified during transaction monitoring.

4.7. Any change in the Customer's risk classification by front-line staff requires written approval from the CO, which shall be based on the justification for the change in risk level.

4.8. Under this Procedure, the following are considered low-risk indicators:

4.8.1. State or local government authorities,

4.8.2. Organizations founded by the state.

4.9. Risk is assessed as Medium (Standard) in cases where neither high-risk nor low-risk indicators are present.

4.10. In accordance with Annex 7 attached to this Procedure, a high-risk rating is determined by the presence of one or more high-risk indicators. The CO is guided by, but not limited to, the following criteria when classifying a Customer as high-risk, taking into account a number of factors, such as:

4.10.1. **Country or geographical risk** – the Customer is located or resides in a:

4.10.1.1. Offshore or tax-privileged jurisdiction,

4.10.1.2. Country subject to international comprehensive sanctions,

4.10.1.3. Country with a high level of corruption (corruption perception index below 30 or with no rating),

4.10.1.4. Country included in the FATF grey list.

4.10.2. **Customer, transaction, or business relationship risk:**

4.10.2.1. The Customer is a PEP (Politically Exposed Person), a family member or a close associate of a PEP,

4.10.2.2. The Customer is a non-resident and the account opening in Armenia lacks clear economic justification,

4.10.2.3. The Customer operates in a sector identified as high-risk from an AML/CFT perspective, as defined in Annex 7 of this Procedure,

4.10.2.4. Transactions conducted by an inactive Customer (no activity for more than one year) that exceed the previously declared transaction volume or frequency by two times or more,

4.10.2.5. The Customer has a record of financial crimes,

4.10.2.6. Customers who engage in frequent and unjustified trading of securities,

4.10.2.7. Mirror trading, which involves two offsetting transactions where bonds or shares are bought in one currency and sold in another.

4.10.3. **Product, service, or delivery method risk:**

4.10.3.1. Establishing a business relationship without face-to-face interaction, where the Customer does not have a bank account and thus has not been previously identified by another financial institution,

4.10.3.2. Transactions related to low-priced securities (penny or microcap stocks),

4.10.3.3. Transactions or business relationships with unusual terms or where the economic or other legitimate purpose is not readily apparent.

4.11. High-risk indicators may also be identified during the Customer Due Diligence (CDD) process. In order to detect and assess such indicators, the CO (Compliance Officer) compares and analyzes the Customer's identification data, business profile, the nature and purpose of transactions, information from publicly available sources, and other relevant circumstances surrounding the transaction.

4.12. The establishment of a business relationship and execution of transactions without face-to-face interaction is not considered a high-risk indicator under this Procedure, as the Company performs online identification in accordance with the procedure defined in Clauses 2.9–2.11. Furthermore, transactions with the Company are carried out exclusively via non-cash means, which implies that the Customer has already been identified by another financial institution. Nevertheless, if a high-risk or suspicious indicator emerges during the course of the business relationship, the CO may reassess the risk level.

4.13. To assess potential and existing ML/TF risks, the CO conducts an annual strategic risk analysis, taking into consideration inherent risks specific to the Company, the internal control system, residual risk, and its management. Based on this analysis, a report is prepared and submitted to the Company's Executive Body/Management/Board (if applicable).

CHAPTER 5. TRANSACTION MONITORING

5.1. In order to detect suspicious transactions, the Compliance Officer (CO) performs transaction monitoring by developing potential scenarios for identifying suspicious activity. These scenarios are based on the indicators and typologies published by the Competent Authority, as well as the Company's risk appetite.

5.2. With respect to the analysis of all types of business relationships and transactions, the CO conducts ongoing monitoring at least semi-annually. The sample segment for monitoring is determined based on the Customer's or business relationship's risk level, without focusing on transaction thresholds. The monitoring aims to identify unusual behavioral patterns in Customer activities, compare transaction history with ongoing transactions and the Customer's business profile, and detect any significant, unusual, or suspicious movement or deviation of funds.

5.3. During the monitoring process, Enhanced Due Diligence (EDD) is carried out for the analysis of high-risk Customers/transactions. In such cases, front-line staff must support the CO in obtaining and collecting the necessary information and/or documents required for the EDD. Enhanced Due Diligence is also conducted when a transaction is performed, processed, or when there is knowledge of the Customer's intention to perform such a transaction. Support actions by front-line employees in the EDD process shall at a minimum include:

5.3.1. Clarifying and obtaining supporting documents (e.g., contracts, bank account statements, and where necessary, notarized copies) regarding the transaction parties, involved third parties (if any), the purpose of the transaction, and the terms of its execution;

5.3.2. Clarifying the source of the Customer's income and wealth by requesting information substantiating their legality (including documents such as income statements, tax declarations, notarized documentation of inheritance or donation, etc.).

5.4. The information and/or documents obtained during the Enhanced Due Diligence (EDD) process shall be submitted to the Compliance Officer (CO), who shall in turn carry out the following:

5.4.1. In conducting analysis related to the transaction or business relationship, the CO shall rely on the necessary information (including additional documents) collected by the front-line employee about the Customer, make use of limited-access and publicly available information sources, and review media coverage;

5.4.2. Make inquiries to a wide range of competent authorities and other reporting entities,

as well as foreign partners;

5.4.3. Conduct identification procedures for the transaction parties, beneficial owner, and authorized person;

5.4.4. When comparing the sources, movement, and volumes of funds circulated through the Customer's various transactions, choose the longest or multiple comparable time periods possible;

5.4.5. Perform multi-level analysis to identify the existence of links between Customers, transactions, and business relationships, including for the purpose of revealing potential indirect connections,

5.4.6. Assess the potential money laundering/terrorism financing (ML/TF) risks in the transaction or business relationship by comparing them with the grounds and indicators of suspicious transactions and business relationships;

5.4.7. Based on the results of the EDD, approve or reject the transaction. In the case of already completed transactions or established business relationships, decide whether to continue or terminate the relationship, apply special conditions, or establish enhanced monitoring over the Customer's transactions for a specific period.

5.5. If, upon comparing the collected information and the Customer's transactions, the CO is convinced of their legality, the transaction or business relationship is approved/performed. In the absence of sufficient justification or the inability to carry out EDD, the CO considers filing a suspicious transaction report.

5.6. The results of transaction monitoring and the EDD—including all information related to rejected and unexecuted transactions or business relationships—shall be documented and retained in accordance with the procedures and timeframes defined by law.

CHAPTER 6. IMPLEMENTATION OF THE CUSTOMER DATA UPDATE PROCESS

6.1. The information collected as part of the Customer Due Diligence process and the updates of the Know Your Customer (KYC) questionnaire (Appendices 1, 2, and 3), excluding the information obtained through identification and verification of the Customer's identity, shall be updated no later than:

6.1.1. once a year — for medium (standard) risk Customers,

6.1.2. every six months — for high-risk Customers,

6.1.3. once every two years — for low-risk Customers

6.1.4. every three months — for Politically Exposed Persons (PEPs).

6.2. The information obtained through the Customer's identification and identity verification shall be updated annually.

6.3. On a quarterly basis, the Compliance Officer prepares a list of Customers subject to data update, in accordance with the deadlines outlined in this chapter, and submits it to the Head of the Customer Service Department for the purpose of organizing the update process.

6.4. The basis for determining the update deadline shall be the date of account opening or establishment of the business relationship. For subsequent updates, the period shall be calculated from the date of the last update, which must be properly recorded.

6.5. In addition to identification data, the KYC questionnaire shall also be updated. For financial institutions, the Wolfsberg Questionnaire and the AML/CFT Policy must also be updated, unless there have been no changes in the institution's structure or in the composition of the executive body/management.

6.6. Customers whose data have not been updated within the deadlines specified in Clause 6.1 of this Procedure shall not be allowed to perform transactions until the data are properly updated.

6.7. The Head of the Customer Service Department shall submit the results of the update process, including information on Customers whose data were not updated, to the Compliance Officer in writing with appropriate documentation.

CHAPTER 7. INDICATORS AND PROCEDURE FOR IDENTIFYING AND REPORTING SUSPICIOUS TRANSACTIONS OR BUSINESS RELATIONSHIPS

7.1. The process of qualifying a transaction or business relationship as suspicious may be initiated either as a result of receiving internal or external signals or at the initiative of the Compliance Officer (CO). The assessment of a transaction or business relationship as suspicious can apply not only to executed transactions and established relationships, but also to attempted transactions or relationship initiations.

7.2. Internal signals refer to alerts submitted to the CO by employees, the Company's management bodies, or other staff members.

7.3. External signals refer to alerts received from the Competent Authority, other regulatory bodies, reporting entities, foreign partners, as well as from both restricted-access and publicly available information sources.

7.4. A transaction or business relationship (hereinafter within this chapter referred to as the Transaction) may be considered suspicious if:

- 7.4.1. The Customer offers or concludes a Transaction through which it is not possible to identify the Customer or obtain the required information,
- 7.4.2. The terms of the Transaction are inconsistent with the Customer's business profile, or with the standard conditions of transactions in the relevant industry or market practice,
- 7.4.3. It becomes evident to the front-line employee that the proposed or concluded Transaction clearly lacks a lawful or economic purpose,
- 7.4.4. Based on its structure and flow (dynamics), the Transaction matches typologies defined in international best practices and guidelines issued by the Central Bank of Armenia,
- 7.4.5. It is evident that the Transaction value is purposefully kept below the statutory threshold in order to avoid the Company's obligation to report to the Central Bank,
- 7.4.6. There is a match between the Customer's or counterparty's identification data and the data of individuals listed as terrorists, sanctioned persons, individuals associated with foreign politically exposed persons (PEPs), or other persons indicated in directives of the Competent Authority.

7.5. In the event of a suspicious or unusual transaction or business relationship, the front-line employee must immediately notify the CO, specifying the suspicious criteria under which the transaction was assessed, in accordance with Appendix 9 to this Procedure.

7.6. The CO reviews the alert and, if necessary, conducts enhanced due diligence and applies relevant restrictions. Based on the analysis, the CO decides whether to submit a Suspicious Transaction Report (STR) to the Financial Monitoring Center (FMC).

7.7. If, based on internal and external signals and/or independent analysis, the CO concludes that the transaction or business relationship is not suspicious and decides not to file an STR, the justifications for this conclusion, the findings, and the analysis performed must be documented and retained in accordance with the law and within the legally defined timeframe.

7.8. The final decision to classify a transaction or business relationship as suspicious is made by the Compliance Officer.

CHAPTER 8. PROCEDURE FOR REPORTING TRANSACTIONS SUBJECT TO MANDATORY NOTIFICATION

8.1. In accordance with the Law, the Company is obligated to submit reports to the Financial Monitoring Center (FMC) regarding transactions subject to mandatory notification. Since the Company's Customers only conduct non-cash transactions, transactions that meet or exceed the

threshold of AMD 20 million are subject to mandatory notification.

8.2. The procedure and deadlines for submitting such transactions are regulated by relevant resolutions of the Central Bank of Armenia (CBA).

8.3. These transactions must be reported by the Compliance Officer (CO) no later than three business days after execution, and must be submitted to the FMC through the Lotus messaging system, established between the CBA and the Company.

8.4. If any inaccuracies in the information regarding mandatory reportable transactions result in failure to submit them within the prescribed deadline, the employee who executed the transaction bears responsibility for the consequences.

8.5. Regardless of the transaction amount, the following transactions are not considered subject to mandatory notification:

8.5.1. Transactions executed between two professional participants in the secondary financial market, acting in their own name and on their own account,

8.5.2. Transactions executed by the Company for its own operational needs in the course of its regular business activities, excluding the purchase of financial assets from its Customers,

8.5.3. Amendments to previously reported transactions with Customers, provided that such changes do not affect the transaction amount or currency.

CHAPTER 9. SUSPENSION, REJECTION OR TERMINATION OF A TRANSACTION OR BUSINESS RELATIONSHIP AND FREEZING OF ASSETS

9.1. The Compliance Officer (CO) may suspend a business relationship or a transaction for up to 5 days if there is a reasonable suspicion of money laundering. In case of a suspicion of terrorist financing, the CO is obligated to freeze the business relationship for 5 days. In such cases, the CO must submit a Suspicious Transaction Report (STR) to the Financial Monitoring Center (FMC).

9.2. If the Authorized Body issues a notification to a law enforcement agency regarding the suspended transaction or business relationship, the suspension period is considered extended by 15 days from the moment of notification. The Authorized Body shall inform the Company accordingly. If an extension beyond 15 days is needed, the law enforcement agency shall notify the Authorized Body within that period. In the absence of such notification, the suspension is lifted.

9.3. If the decision to suspend a transaction or business relationship is made by the Authorized Body, the CO shall execute the instruction immediately upon receipt.

9.4. Suspension of a transaction is considered either refusal to execute or temporary restriction until an appropriate decision is received from the Authorized Body.

9.5. The CO must reject or terminate the establishment of a business relationship or the execution of a transaction if a written instruction is received from the Authorized Body, or the Customer refuses to submit the required identification documents, preventing proper due diligence from being conducted.

9.6. In case of rejection or termination of a transaction or business relationship, the CO shall assess the need to file an STR to the Authorized Body.

9.7. In the event of a full match with the UN Sanctions Lists, or immediately upon receipt of an appropriate instruction from the Authorized Body, the CO shall freeze all assets of persons related to terrorism or the proliferation of weapons of mass destruction, and shall restrict any movement on their accounts. Opening of new accounts for such individuals is strictly prohibited.

9.8. The UN Sanctions Lists related to terrorism are published on the Central Bank of Armenia's official website. The CO is responsible for checking for any matches. If a match is found, the CO shall make an independent decision to freeze the assets and immediately report to the Authorized Body by submitting an STR.

9.9. A freeze decision may only be lifted based on a written notice from the Authorized Body
9.10. The final decision regarding the suspension or freezing of a transaction or business relationship is made by the Compliance Officer.
9.11. In the report submitted to the Company's Executive Body/Management Board, the CO must include information on all suspended, frozen, or rejected transactions or business relationships.

CHAPTER 10. COMPLIANCE WITH INTERNATIONAL SANCTIONS REQUIREMENTS

10.1. International organizations periodically publish sanctions lists that impose restrictions or prohibitions on specific countries, individuals, entities, and financial transactions. Such transactions may be subject to freezing, blocking, or suspension.
10.2. The Company recognizes and adheres to sanctions imposed by major international institutions such as FATF, the UN Security Council, the European Union (EU), and the Office of Foreign Assets Control (OFAC).
10.3. The Company's Internal Monitoring Unit assesses the risks of sanctions specific to the Company's business profile and develops mitigation mechanisms, including:
  10.3.1. Periodically reviews the client base by countries of residency and geographic location, as defined by internal regulations. The CO applies enhanced KYC measures to facilitate proper identification of customers subject to sanctions.
  10.3.2. Prior to the launch of new products/services, an analysis is conducted to identify any associated sanctions risks and to design appropriate controls.
  10.3.3. The Company's marketing strategy is developed to avoid targeting individuals or businesses from sanctioned countries, or those with ties to such jurisdictions, thereby mitigating the risk of sanctions violations, circumvention, and reputational damage.
10.4. Daily monitoring of international sanctions is performed by the CO and front-line employees, covering all products and services, regardless of the customer's nationality, transaction type, origin of funds/assets, or jurisdiction of service delivery.
10.5. Prior to onboarding a new client, the CO checks the full name of the individual, and in the case of legal entities, the names of shareholders and beneficial owners, against the sanctions lists. Any potential match is reviewed by the CO, who determines whether the match is a true positive and subsequently approves or rejects the business relationship.
10.6. Following any new sanctions publication, the CO screens the entire existing client base for matches. Additionally, monthly screenings are conducted to ensure no sanctioned individuals or entities are present in the client base.
10.7. The results of sanctions list screening are exported from a restricted-access database in PDF format and retained in accordance with the requirements of the law and internal procedures.
10.8. If a positive match is identified, the CO rejects the transaction or the establishment of a business relationship with the respective individual/entity. This applies equally to legal entities in which a sanctioned person owns 50% or more of the shares or is a beneficial owner.
10.9. If a sanctioned individual or entity is identified among existing clients, the CO immediately issues a blocking instruction to the Company's servicing bank, requesting the freezing of all assets held in the client's accounts. The freezing is executed without prior notice to the client, and a Suspicious Transaction Report (STR) is simultaneously submitted to the Financial Monitoring Center. At the same time, steps are taken to terminate the business relationship with the client.
10.10. All business relationships or transactions that have been suspended or rejected due to sanctions list matches are registered and documented by the Compliance Officer.

CHAPTER 11. CORRESPONDENT OR SIMILAR RELATIONSHIPS WITH FINANCIAL INSTITUTIONS

11.1. When establishing correspondent or other similar relationships with financial institutions, the Compliance Officer (CO) shall conduct proper due diligence to assess the nature of the partner institution’s activities, its business reputation, whether there are any ongoing proceedings related to AML/CFT violations, and to evaluate the institution’s AML/CFT control framework.
11.2. To perform due diligence, the front-line employee sends the "Know Your Customer (KYC) Questionnaire for Financial Institutions" (Annex 6 to this Procedure) to the counterparty institution, along with a request for the documents listed in Annex 3. The collected information and documents are forwarded to the CO for further verification and assessment.
11.3. The CO shall also confirm that, in the case of omnibus accounts or accounts opened for third-party (non-proprietary) funds, the foreign financial institution applies appropriate due diligence measures to its own clients and is capable of providing information on such due diligence upon request.
11.4. If the submitted documentation is complete and there are no clarification requests, the CO shall complete the due diligence process within no more than three (3) business days and share the results with the requesting department.
11.5. The Company prohibits establishing or maintaining correspondent or similar relationships with shell companies, and also prohibits the use of the Company’s services by such entities.

CHAPTER 12. FUNCTIONS OF THE INTERNAL MONITORING BODY AND CONDUCT OF AUDIT

12.1. In accordance with Clause 2.5 of the Company’s Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Policy, the Compliance Officer (CO) shall submit a semiannual report to the Executive Body and/or the General Meeting of Participants, which shall at a minimum include:
  12.1.1. The number of transactions subject to mandatory reporting,
  12.1.2. The number and brief descriptions of suspicious transactions or business relationships,
  12.1.3. The number and summary of transactions or business relationships analyzed but not reported as suspicious,
  12.1.4. The number and brief descriptions of transactions or relationships that were suspended or rejected,
  12.1.5. The value of suspended transactions,
  12.1.6. The amount of frozen funds,
  12.1.7. Other issues and information related to AML/CTF activities,
  12.1.8. Any additional information requested by the Executive Body or Management of the Company.
12.2. In accordance with the law, the Internal Audit shall conduct inspections at least once per year to ensure that the Executive Director and the CO ensure full compliance of the Company's operations with the requirements of the Law, regulatory legal acts of the Competent Authority, the Policy, this Procedure, and other internal legal acts.
12.3. Following the audits, the Internal Audit shall submit a report with its findings and assessments to the Executive Body / Management (with a copy to the Executive Director), including conclusions on the adequacy and effectiveness of AML/CTF and sanctions-related staff training and education.
12.4. If, during scheduled or unscheduled audits of any structural unit, the Internal Audit detects suspicious transactions, potential money laundering schemes, or violations of internal or external legal requirements, it must inform the CO before submitting the final audit report to the relevant competent body, to allow the timely implementation of AML/CTF measures.

CHAPTER 13. TRAINING OF EMPLOYEES IN THE FIELD OF AML/CFT AND SANCTIONS COMPLIANCE

13.1. The Compliance Officer (CO) shall organize annual training for frontline employees, Internal Audit, the Executive Body, Participants, and other staff responsible for AML/CFT and international sanctions compliance and prevention.
13.2. Training for newly hired employees shall be conducted within three months from the date of employment.
13.3. Training materials, participant data, and attendance records shall be documented and retained for a period of five years.
13.4. Training programs, all related materials, as well as names and signatures of participants, shall be recorded in accordance with Appendix 8 ("Training/Refresher Course Log on AML/CFT and Sanctions Compliance") and kept by the CO for at least five years.
13.5. If the training or refresher course is organized by a third-party organization, the employee who participated shall submit the documentation specified in Clause 13.4 to the CO as soon as possible after completing the course.

CHAPTER 14. COLLECTION, RECORDING, AND RETENTION OF INFORMATION

14.1. he receipt and collection of information related to a transaction or business relationship shall be carried out in the course of its execution. Information is collected by frontline staff, relevant departments involved in the transaction, and, in cases where the information is solely accessible to the Compliance Officer (CO), it is collected by the CO.
14.2. Information shall be obtained from Clients, transaction participants, external sources, and information databases.
14.3. The collected information may be recorded either in paper or electronic format, and the recording is performed by the entity or individual possessing the information.
14.4. The Client's personal file folder, opened under the Client's name, shall include complete and filled-out copies of documents necessary for identification, verification of identity, the "Know Your Customer" questionnaire, and other collected documents.
14.5. The attached information must be authentic, complete, and up to date.
14.6. The Company shall retain the following information:
    14.6.1. The Client's identification data;
    14.6.2. All necessary data regarding domestic and international transactions or business relationships (including the name of the Client and the counterparty, registration address (if available), residence (or location), nature of the transaction, date of execution, amount and currency, and, where applicable, the type and number of the account), sufficient to reconstruct the full picture of the transaction or business relationship and/or to reveal the true nature of the business relationship;
    14.6.3. Any other information and documents that become available to the Company in the course of the transaction or business relationship.
14.7. The retention period for the information is five years, as prescribed by law.

CHAPTER 15. LIABILITY

15.1. In case of violations of the requirements established by this Procedure and the Policy on Combating Money Laundering and Terrorism Financing, the Executive Director may impose disciplinary or other measures of liability on the heads and employees of the Company's departments, as prescribed by the legislation of the Republic of Armenia and internal legal acts.
15.2. Heads of the Company's departments shall be held liable for the inaccuracy, untimeliness,

incompleteness, and/or unreliability of the data provided to the Compliance Officer, as required under this Procedure and the Policy on Combating Money Laundering and Terrorism Financing, whether the data was submitted by them personally or by their staff.

15.3. The Company or its employees (including its managers) shall not be subject to criminal, administrative, civil, or other liability for the proper performance of their duties as stipulated by the Law.

CHAPTER 16. MISCELLANEOUS PROVISIONS

16.1. This Procedure enters into force upon its approval.

16.2. The Appendices to the Procedure, as well as any other documents arising from the implementation of this Procedure, shall be approved by the Executive Body/Board of Directors. Any amendment or adoption of such documents shall not be considered a revision of the Procedure itself.

16.3. The Compliance Officer of the Company shall be considered the owner of this Procedure.

16.4. The Compliance Officer shall have direct and immediate access to all information (including documents) obtained and maintained by the Company as prescribed by applicable legislation and this Procedure, for the purpose of overseeing transactions and/or business relationships in the context of AML/CFT.

16.5. In the event of future amendments and/or supplements to the applicable legislation, the Company shall adhere to those changes even before this Procedure is formally updated to reflect the new legal requirements.

16.6. Within one week following the approval of this Procedure, it shall be submitted to the Central Bank of Armenia through the CBANet system.