

*Approved by the Supervisory  
Board of IBA OJSC.  
Protocol № 19; Decision № 19;  
Date: 17.12.2021*

**POLICY**  
**of IBA OJSC**  
**On the Prevention of the Legalization of Criminally Obtained  
Funds or Other Property and the Financing of Terrorism**

**Contents**

|   |    |
|---|----|
| 1. General Provisions .....   | 2  |
| 2. Basic definitions .....  | 2  |
| 3. The purpose of the Policy .....  | 4  |
| 4. Principles of the Policy .....   | 4  |
| 5. Areas of activity .....  | 6  |
| 6. Organization of activities on the prevention of the legalization of criminally obtained funds or other property and the financing of terrorism ..... | 6  |
| 7. Participants of the Policy .....   | 7  |
| 8. The Bank's program on the prevention of the legalization of criminally obtained funds or other property and the financing of terrorism .....         | 8  |
| 9. Control over sanctions requirements .....  | 9  |
| 10. Liability .....   | 9  |
| 11. Reporting .....   | 10 |
| 12. Final Provisions .....  | 10 |

## 1. General Provisions

- 1.1. This Policy is developed based on the Laws of the Republic of Azerbaijan “On Banks”, “Law of the Republic of Azerbaijan On the Prevention of the Legalization of Criminally Obtained Funds or Other Property and the Financing of Terrorism”, “Compliance Policy of the International Bank of Azerbaijan”, Normative legal documents of the Financial Monitoring Service of the Republic of Azerbaijan, as well as the recommendations of the Financial Action Task Force (FATF) of the Organization for Economic Cooperation and Development, the principles of the Basel Committee on Banking Supervision and the "Wolfsberg Principles" widely used in banking practice.
- 1.2. The employees of the Bank who work directly with customers or are involved in liaising with them must apply the provisions of this Policy in the performance of their duties.

## 2. Basic definitions

- 2.1. The definitions used in this Policy shall have the following meanings:
  - 2.1.1. **legalization of criminally obtained funds or other property** – conversion or transfer of funds or other property, knowing that such funds or other property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the funds or other property or of helping any person who is involved in the commission of any crime to evade the legal consequences of his or her action, or accomplishment of financial transactions or other deals for the same purposes by using funds or other property, knowing that such funds or other property is the proceeds of crime; or the concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to funds or other property, knowing that such funds or other property is the proceeds of crime;
  - 2.1.2. **financing of terrorism** – willful provision or collection funds or other property by any means, in full or in part, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used in order to finance preparation, organization and carrying out actions envisaged in the relevant articles of the Criminal Code of the Republic of Azerbaijan by a person or a group (organization, community) or an individual terrorist or a terrorist group (organization, community);

- 2.1.3. **criminally obtained funds or other property** – funds of every kind, property, whether movable or immovable, corporeal or incorporeal, tangible or intangible, legal documents evidencing the title to such property, obtained directly or indirectly through the commission of an offence provided by the Criminal Code of the Republic of Azerbaijan;
- 2.1.4. **virtual asset** - a digital expression of value that can be sold or transferred digitally, used as a means of exchange for payment or investment purposes;
- 2.1.5. **transactions with funds or other property** – transactions aimed at acquisition, exercising, change or termination of civil rights to the funds and/or other property as a result of transactions with them;
- 2.1.6. **AML / CFT** – Prevention of the legalization of criminally obtained funds or other property and the financing of terrorism;
- 2.1.7. **internal control over AML / CFT** – comprehensive internal control measures of the Bank to detect the operations to be monitored and other operations related to the legalization of criminally obtained funds or other property and the financing of terrorism, as defined by law;
- 2.1.8. **customer** – natural or legal person who permanently or irregularly uses any of the Bank's services in carrying out transactions with funds or other property;
- 2.1.9. **structural unit** – the relevant unit of the Bank, which carries out transactions with customers or establishes relations with them in the performance of its functions;
- 2.1.10. **responsible structural unit** – Responsible structural unit of the Bank carrying out activities in the field of financial monitoring;
- 2.1.11. **responsible person of the bank** - the person appointed on the basis of the decision of the Board of Directors, who is responsible for monitoring the implementation of internal rules and procedures for the prevention of legalization of criminally obtained funds or other property and financing of terrorism in the Bank, the exchange of information with the FMSRA, as well as preparing and submitting relevant reports on the transactions to be monitored;
- 2.1.12. **responsible person** – the person appointed by the order of the Chairman of the Board of Directors, who is responsible for monitoring the implementation of internal rules and procedures for the prevention of legalization of criminally obtained funds or other property and financing of terrorism in the structural unit of the Bank, the exchange of information with the responsible structural unit of the Bank, as well as preparing and submitting relevant reports on the transactions to be monitored;

- 2.1.13. **program** – comprehensive measures aimed at preventing the use of the Bank and its resources as a tool in the legalization of criminally obtained funds or other property and the financing of terrorism (internal rules and procedures, responsible person, conducting trainings, internal audit, etc.);
  - 2.1.14. **screening** - checking the names of persons and identified words on the relevant lists through special information search databases;
  - 2.1.15. **sanction lists** – Lists of individuals or legal entities subject to sanctions in accordance with the legislation of the Republic of Azerbaijan and international agreements to which Republic of Azerbaijan is a party, with relevant resolutions of the United Nations Security Council and the European Union, with the Decisions of the US Treasury Department's Office of Foreign Assets Control (OFAC) within the AML / CFT, as well as relevant lists established by the Bank in accordance with the procedure established by the relevant executive authority;
  - 2.1.16. **FMSRA** – Financial Monitoring Service of the Republic of Azerbaijan exercising relevant powers in the field of prevention of legalization of criminally obtained funds or other property and financing of terrorism.
- 2.2. The definitions set forth in this article are used only for the purposes of this Policy.
  - 2.3. Other definitions used in this Policy have the meanings defined by the existing legislative acts of the Republic of Azerbaijan.

### **3. The purpose of the Policy**

- 3.1. The purpose of this Policy is to determine the principles, main directions, participants of intra-bank activities on AML / CFT, to prevent the use of the Bank as a tool in legalization of criminally obtained funds or other property and financing of terrorism, including to detect internal bank violations in relation to AML / CFT.

### **4. Principles of the Policy**

- 4.1. The Bank's activities in the field of AML / CFT are based on the following principles:
- 4.2. The principle of legislation
  - 4.2.1. The legislation of the Republic of Azerbaijan and the requirements established by international agreements to which the Republic of Azerbaijan is a party, in the field of AML / CFT are observed
- 4.3. Know your customer principle
  - 4.3.1. The activities of existing and potential customers are thoroughly analyzed, the documents submitted by them are registered, checked and additional information is collected to minimize the Bank's involvement in the scheme of

suspicious, complex, large-scale unusual financial transactions carried out by individual customers. This activity:

- 4.3.1.1. is based on the lawful and conscientious conduct of commercial activities;
- 4.3.1.2. increases vigilance of the Bank's employees against any suspicious transactions, especially the transactions of a customer about activities of whom there is information incompatible with the Bank's activities;
- 4.3.1.3. is aimed at timely detection of suspicious transactions of customers.

#### 4.4. Principle of moratorium

- 4.4.1. Establishment, continuation of business relations or conducting operations with customers is refused in the following cases:
  - 4.4.1.1. if there are reasonable doubts about the customer's involvement in the legalization of criminally obtained funds or other property and financing of terrorism;
  - 4.4.1.2. if there are reasonable doubts about the customer's involvement in transnational organized crime, as well as in support of armed separatism, extremism and mercenaries, illicit trafficking in drugs and psychotropic substances;
  - 4.4.1.3. if the financial institution does not take full measures in the field of AML / CFT;
  - 4.4.1.4. if the financial institution does not have a physical presence in any state or territory where it is registered and is not covered by regulatory and supervisory processes by the banking regulatory / supervisory authorities ("shell bank");
  - 4.4.1.5. when the customer conducts transactions that do not have a clear economic or legal purpose;
  - 4.4.1.6. if the names of the customer, its beneficiaries and parties to the transactions are included in the sanctions lists;
  - 4.4.1.7. In case of business relations or transactions with individuals or legal entities of states included in the list developed by the relevant body and determined by the Bank's internal policy ("high-risk customers") in the field of AML / CFT, taking into account the exceptions determined by the decision of the Board of Directors;
  - 4.4.1.8. if the customer does not submit the necessary documents or submits false documents, as well as deliberately submits incorrect information.

- 4.4.2. The transactions referred to in sub-clause 4.4.1 of this Policy are suspended for the purpose of investigating them with the participation of customers.
- 4.4.3. Opening of accounts under anonymous and fictitious names, as well as issuance of anonymous certificates of deposit are denied.

## **5. Areas of activity**

- 5.1. The main areas of activity of the Bank in the field of AML / CFT include the following:
  - 5.1.1. to carry out continuous and purposeful work to achieve the objectives of this Policy;
  - 5.1.2. Participation of Bank employees in AML / CFT work;
  - 5.1.3. Improving the professionalism of employees in AML / CFT work, organizing training and checking the level of knowledge;
  - 5.1.4. Improving existing intra-bank regulatory documents on AML / CFT and developing new ones;
  - 5.1.5. Regular updating of internal control rules in the field of AML / CFT in accordance with the existing changes in the legislation of the Republic of Azerbaijan, legal acts of the Central Bank of the Republic of Azerbaijan and FMSRA;
  - 5.1.6. Application of new mechanisms in AML / CFT in Banking practice;
  - 5.1.7. Creating a single information space where the structural units dealing with AML / CFT issues can analyze and monitor with the help of software and hardware used in the bank.

## **6. Organization of activities on AML / CFT**

- 6.1. The Bank establishes internal control activities on AML / CFT as follows:
  - 6.1.1. The Board of Directors appoints a responsible person of the Bank in order to create an effective system in the field of AML / CFT and prevent the involvement of the Bank in the legalization of criminally obtained funds and in financing of terrorism as a result of banking transactions conducted or intended by the customer;
  - 6.1.2. The Chairman of the Board of Directors appoints the responsible person in the structural units of the Bank;
  - 6.1.3. The responsible person of the Bank reports to the Board of Directors on the results of the implementation of the Bank's internal control program for AML / CFT purposes;
  - 6.1.4. The Bank's internal audit department regularly monitors compliance with AML /

CFT legislation and assesses the adequacy of the internal control system in this area;

- 6.1.5. Organization of activities on the prevention of the legalization of criminally obtained funds or other property and the financing of terrorism is controlled by the Board of Directors.

## **7. Participants of the Policy**

- 7.1. The main participants in the process of ensuring the Bank's activities in the field of AML / CFT are as follows:
  - 7.1.1. Supervisory board;
  - 7.1.2. Board of Directors;
  - 7.1.3. Responsible structural unit;
  - 7.1.4. Responsible person of the bank;
  - 7.1.5. Responsible person;
  - 7.1.6. Employees of the structural unit.
- 7.2. Supervisory board:
  - 7.2.1. Determines the Bank's AML / CFT policy;
  - 7.2.2. Executes general control over the compliance of intra-bank rules in the implementation of this Policy;
  - 7.2.3. Develops and implements an internal control system for AML / CFT.
- 7.3. Board of Directors:
  - 7.3.1. Ensures the implementation of this Policy;
  - 7.3.2. Within the scope of its authority, adopts internal normative documents arising from the objectives of this Policy, as well as ensures their implementation
- 7.4. Responsible structural unit:
  - 7.4.1. Carries out monitoring in the field of AML / CFT, obtains, collects and analyzes information on the transactions detected during monitoring and those who carried them out, as well as takes necessary measures in accordance with this information;
  - 7.4.2. Detects relevant offenses in the field of AML / CFT, prevents their commission;
  - 7.4.3. Prepares intra-bank training materials on AML / CFT;
  - 7.4.4. Carries out other relevant activities within its competence to achieve the objectives of this Policy.
- 7.5. Responsible person of the bank:
  - 7.5.1. Supervises the implementation of internal rules and procedures on AML / CFT

in the Bank;

- 7.5.2. Exchanges information with FMSRA;
  - 7.5.3. Prepares relevant reports on operations to be monitored and submits them accordingly;
  - 7.5.4. Develops intra-bank training program on AML / CFT;
  - 7.5.5. Carries out other activities arising from this within its competence to achieve the objectives of this Policy.
- 7.6. Responsible person:
- 7.6.1. Supervises the implementation of internal rules and procedures on AML / CFT in the structural unit;
  - 7.6.2. Exchanges information with the responsible structural unit;
  - 7.6.3. Prepares relevant reporting forms related to the operations to be monitored and submits them accordingly;
  - 7.6.4. Supervises the participation of employees of the structural unit in the assigned intra-bank trainings on AML / CFT;
  - 7.6.5. Carries out other activities arising from this within its competence to achieve the objectives of this Policy.
- 7.7. Employees of the structural unit:
- 7.7.1. Comply with the requirements of the legislation in the field of AML / CFT, intra-bank regulations.
- 7.8. The participants mentioned in sub-clauses 7.1.1–7.1.6 of this Policy perform other functions arising from the legislation and this Policy within their authority to ensure the Bank's activities in the field of AML / CFT.

## **8. The Bank's program on the prevention of the legalization of criminally obtained funds or other property and the financing of terrorism**

- 8.1. The Bank's action program in the field of AML / CFT consists of the following elements:
  - 8.1.1. internal rules for identification and verification of customers and beneficiaries;
  - 8.1.2. Criteria (indicators) for the detection of cases and transactions (including virtual assets<sup>1</sup>) that provide sufficient grounds to suspect they are related to the

---

<sup>1</sup> Digital exchange of national and foreign currency, shares and other financial instruments is not considered a virtual asset.



- terrorism;
- 8.1.3. criteria (indicators) for detecting transactions to be monitored;
  - 8.1.4. rules for detection, prevention of suspicious transactions and submission of information to FMSRA;
  - 8.1.5. procedures for establishing business relations with customers, conducting transactions and regularly updating customer data, as well as monitoring compliance with relevant requirements on sanctions lists during the inspection of the customer base;
  - 8.1.6. procedures for submitting to the relevant state body the information required in accordance with the international agreements to which the Republic of Azerbaijan is a party on financial transactions carried out by individuals or legal entities of foreign countries;
  - 8.1.7. rules for documenting information and ensuring confidentiality;
  - 8.1.8. procedures for recruitment and inspection of employees;
  - 8.1.9. rules for conducting trainings on AML / CFT;
  - 8.1.10. to take regular measures to check and, if necessary, update the procedures and rules included in the program in order to ensure their relevance;
  - 8.1.11. internal audit.

## **9. Control over sanctions requirements**

- 9.1. The Bank organizes inspection measures specified in sub-clauses 8.1.1, 8.1.5 and 8.1.8 of this Policy and monitor the implementation of work on these measures.
- 9.2. The Bank takes necessary measures to automate and constantly improve the screening process.
- 9.3. The Bank establishes a reporting system on compliance or suspicious transactions detected during the screening process and monitor its effective operation.

## **10. Liability**

- 10.1. The responsible person of the Bank exercising control over the implementation of the measures defined by this Policy and other employees of the Bank implementing those measures shall be responsible.

## **11. Reporting**

- 11.1. The responsible structural unit prepares a report on AML / CFT activities at least once a quarter and submits it to the Board of Directors. The report covers at least the following:

- 11.1.1. information on the work done during the reporting period and analysis;
  - 11.1.2. statistics;
  - 11.1.3. information on conducted trainings;
  - 11.1.4. information on revealed discrepancies related to the implementation of the requirements set forth in the intra-bank regulations arising from this Policy.
- 11.2. The Board of Directors reviews the submitted report and submits it to the Supervisory Board for consideration.

## **12. Final Provisions**

- 12.1. This Policy shall enter into force upon approval by the Supervisory Board of the Bank.
- 12.2. Any additions and changes to this Policy can be made by the decision of the Supervisory Board.