Approved by the Supervisory Board of "ABB" OJSC.
Protocol No. 6; Resolution No. 14; Date: 22.02.2023

POLICY

"Know Your Customer" on the activities in the field of fighting the legalization of criminally obtained property and financing the terrorism of "ABB" OJSC

Table of contents

1. General provisions

1.1 This Policy is based on the Laws of the Republic of Azerbaijan "On Banks", "On Combating Legalization of Criminal Property and Financing of Terrorism" and "On Targeted Financial Sanctions", “Requirements for the organization of internal control systems for activities against the legalization of money or other property obtained through criminal means and the financing of terrorism of monitoring participants who are legal entities and other persons participating in monitoring" of the Financial Monitoring Service of the Republic of Azerbaijan, Methodological Guidance on "Know Your Customer Policy" "On activities of monitoring participants and other persons involved in monitoring in the field of combating money laundering and terrorist financing and other legal acts, as well as the recommendations of the Financial Action Task Force (FATF), the principles of the Basel Committee on Banking Supervision and the "Wolfsberg Principles" and determines the purpose and main elements of the complex system of measures related to the process of collecting necessary information about existing and potential customers, verifying their identity and the source of their property in an appropriate manner by "ABB" OJSC (hereinafter - Bank).

1.2 This Policy covers the relevant employees of the Bank working directly with customers or participating in establishing relations with them, arising from the performance of their functional duties.

2. Basic concepts

2.1. The terms used in this Policy have the following meanings:

2.1.1. **KYC**[1] – Bank's activities in the field of "Know Your Customer";

2.1.2. **LP/FT –** legalization of property obtained through crime and financing of terrorism;

2.1.3. **FLP/FT –** fight against the legalization of property obtained through crime and the financing of terrorism;

2.1.4. **FLP/FT Law -** Law of the Republic of Azerbaijan "On the fight against the legalization of property obtained through crime and the financing of terrorism";

2.1.5. **customer –** an individual or foreign legal entity using any of the Bank's services;

2.1.6. **beneficial owner** – person who ultimately exercises control over the customer or who is the real owner of the customer, who is a legal entity or foreign legal entity, and (or) for whom benefit transactions are conducted, as well as the physical person (persons) who ultimately exercises effective control over the legal entity or foreign legal institution;

[1] In international terminology – “Know Your Customer”

2.1.7. **suspect transactions** – transactions creating suspicion that the property is related to LP/FT or sufficient grounds for such suspicion;

2.1.8. **unusual transactions** – transactions being not typical for the current activity of the customer, are complex, unusually large-scale, as well as transactions not having an obvious economic or legal purpose;

2.1.9. **virtual asset** – a digital expression of value acting as a medium of exchange for payment or investment purposes and existing in the virtual asset circulation system[2];

2.1.10. **identification** – determination of the identity, legal capacity, representative authority and business activity of the customer, beneficial owner and representative;

2.1.11. **additional identification** – verification of accounts and business relationships or clarifying the purpose of transaction and the essence of transaction by other methods, studying the shareholders of the customer being a legal entity and their participation shares, obtaining more accurate information about the customer, beneficial owner and the source of the property (if possible) through other reliable sources and their confrontation;

2.1.12. **verification** – determining the authenticity of the identification data obtained about the customer, beneficial owner and authorized representative through reliable sources;

2.1.13. **high-risk zones** – the list of states or territories not having an adequate fighting system, supporting armed separatism, extremism, hired work and terrorist activities, not requiring the disclosure of identification data and documents during financial transactions and being subject to sanctions or other similar measures by international organizations identified on the basis of reliable sources (mutual assessment or detailed reports published by international organizations and institutions, as well as progress reports) in the field of combating the legalization of criminally acquired property and the financing of terrorism, posted on the official website of FMSRA

2.1.14. **sanctions list** – the list of persons to be sanctioned by the Law "On Targeted Financial Sanctions" of the Republic of Azerbaijan, European Union (EU) Sanctions, sanctions of the Office of Foreign Assets Control (OFAC) of the US Ministry of Finance;

2.1.15. **control list** – lists of persons kept under control by the financial market control body and the Bank;

[2] The digital equivalent of national and foreign currency, securities, as well as derivative financial instruments are not considered virtual assets

2.1.16. **customer profile** – such a set of characteristic features as identification data, the customer's country of origin, important social position and social status currently or previously held by the customer, financial situation, on whose behalf he/she acts, related accounts, business activity and its nature, location and so on;

2.1.17. **respondent bank** – the bank in whose favor the correspondent account was opened;

2.1.18. **Shell type company** – a company existing only on paper, not having its own personal assets and operations (including companies having no office or employees), having only a bank account, obtaining a controlling stake or acting as a front for illegal business purposes (tax evasion and so on) or as an instrument for raising cash before starting operations;

2.1.19. **accountable manager** – a member of the Board of Directors of the Bank or the general director responsible for the activity of the responsible structural unit;

2.1.20. **person in charge of the bank** – A person appointed on the basis of the decision of the Board of Directors of the Bank and being responsible for monitoring the implementation of internal rules and procedures for anti-LP/FT activities in the Bank, for exchanging information with FMSRA, as well as for preparing and submitting relevant reports on to be monitored operations;

2.1.21. **person in charge of the CCS** – The person appointed by the order of the Chairman of the Board of Directors of the Bank and being responsible for monitoring the implementation of internal rules and procedures for anti-LP/FT activities in CCS, exchanging information with the responsible structural unit, as well as preparing relevant reports on operations to be monitored and submitting them accordingly;

2.1.22. **political persons of influence** – persons holding an important state or public position in any state (territory) or international organization or previously held such a position[3], their family members and close relatives;

2.1.23. **FMSRA** – the Financial Monitoring Service of the Republic of Azerbaijan, a public legal entity exercising relevant powers in the field of combating the legalization of property obtained through crime, as well as the fight against terrorism, terrorist financing, the proliferation of weapons of mass destruction, and the financing of the proliferation of weapons of mass destruction;

[3] Heads of state and government, heads of state bodies (institutions), their deputies, members of the legislative body, members of governing bodies of political parties, judges of the supreme and constitutional courts, members of supervisory bodies and central banks, extraordinary and authorized ambassadors, temporary business lawyers, high military and high special rank persons, members of management bodies of state enterprises, heads of international organizations, their deputies, members of management bodies

2.1.24. **responsible structural unit** – responsible structural unit performing activities in the field of financial monitoring of the Bank;

2.1.25. **CCS** – Branches, departments and Customer service department of the bank.

2.2. The terms mentioned in this article are used only for the purposes of this Policy.

2.3. Other concepts used in this Policy express the meanings defined by the current legislative acts of the Republic of Azerbaijan.

3. Purpose of the policy

3.1. The main purpose of this Policy is a comprehensive analysis of the activities of the customers of the Bank, obtaining detailed information about their business profiles, as well as a comprehensive analysis of the activities of the existing and potential customers of the Bank, obtaining detailed information about their business profiles, recording, checking and separating the documents submitted by them, formation of an action mechanism to minimize the involvement of the Bank in the scheme of suspicious, complex, large-scale unusual financial transactions carried out by individual customers.

4. Basic principles of the policy

4.1. The KYC activity of the Bank is based on the following principles:

4.1.1. Legality – the legislation of the Republic of Azerbaijan in the FLP/FT field and the requirements established by the international agreements supported by the Republic of Azerbaijan are observed;

4.1.2. Transparency - the investigation of the submitted data is detailed, impartial and transparent;

4.1.3. Responsibility – Bank employees are attentive to any suspect and unusual transactions carried out by customers contradicting with the Bank's activities;

4.1.4. Restrictions and "zero tolerance" - in order to prevent violations of local legislation, as well as international standards, the Bank establishes business relations with identifiable and verifiable customers who use banking services for legal purposes, imposes restrictions on blacklisted countries (territories), operations conducted from such states (territories) in accordance with relevant internal regulations, as well, imposes sanctions, controls and demonstrates zero tolerance for customers whose name is on the international "Persons to be Sanctioned" lists and their transactions.

5. Policy participants and their duties

5.1. The followings are the main participants in the process of ensuring the KYC activities of the Bank:

5.1.1. Supervisory board;

5.1.2. Board of Directors;

5.1.3. Person in charge of the bank;

5.1.4. Person in charge of the CCS;

5.1.5. responsible structural unit.

5.2. Supervisory board:

5.2.1. defines "Know Your Customer" Policy of the Bank;

5.2.2. carries out general control over compliance with the internal rules of the bank in the direction of the implementation of this Policy;

5.2.3. approves the internal control system based on the "Know Your Customer" principle.

5.3. Board of Directors:

5.3.1. ensures the implementation of this Policy;

5.3.2. ensures the implementation of the internal control system on the principle of "know your customer";

5.3.3. accepts internal bank regulatory documents arising from the objectives of this Policy within their powers and ensures the implementation of those documents.

5.4. Person in charge of the bank:

5.4.1. Manages the responsible structural division of the bank;

5.4.2. monitors the implementation of internal rules and procedures for KYC in the bank;

5.4.3. submits relevant reports prepared on transactions to be monitored;

5.4.4. supervises the development and implementation of the internal bank training program on KYC;

5.4.5. performs other activities arising from it to achieve the goals of this Policy within his powers.

5.5. Person in charge of the CCS:

5.5.1. monitors the implementation of internal rules and procedures on the "Know Your Customer" principle in CCS;

5.5.2. exchanges information with the responsible structural unit;

5.5.3. supervises the participation of the employees of the CCS where he works, in the internal trainings of the bank appointed according to the principle of "know your customer";

5.5.4. performs other activities arising from this to achieve the goals of this policy within his powers.

5.6. Responsible structural unit:

5.6.1. performs monitoring over KYC, obtains information about suspect and unusual transactions discovered during monitoring and the persons carrying them out, collects and analyzes such information, as well as takes necessary measures in accordance with them;

5.6.2. develops an internal control system based on the "Know your customer" principle;
5.6.3. prepares the internal bank training program on KYC;
5.6.4. detects relevant offenses within KYC and prevents them from being committed;
5.6.5. prepares internal bank training materials on KYC;
5.6.6. performs other relevant activities arising from this to achieve the objectives of this Policy within its powers.

5.7. The participants mentioned in clause 5.1 of this Policy also perform other functions necessary within the framework of their powers to ensure the activities of the Bank in the field of KYC, arising from the legislation and this Policy.

6. Basic provisions of activity in the field of KYC

6.1. The main directions of activity in the field of KYC are as follows:
6.1.1. collecting customer identification data, determining the purpose and essence of business relations, creating a customer profile;
6.1.2. identification and verification of customers and beneficial owners;
6.1.3. conducting risk-based assessment of customers and transactions;
6.1.4. strengthening the knowledge and skills of the Bank's employees in the field of LP/FT.

6.2. The following measures are taken in order to establish business relations with the customer:

6.2.1. The customer's country of origin, current or previous important public position and social status, financial situation, the person on whose behalf they act, related accounts, business activities and their nature, location and other such risk criteria are defined in order to create a customer database and customer profile in accordance with internal bank regulations;

6.2.2. An assessment is made in accordance to the risk criteria mentioned in subsection 6.2.1 of this Policy;

6.2.3. A decision is made to establish business relations with the customer on the basis of the results of the risk assessment.

6.3. Identification and verification measures are taken in relation to the custimers in the following manner in order to establish business relations with them:

6.3.1. before establishing business relations;
6.3.2. before any one-time operation[4] expected to be carried out within or more than the limits[5] set by the legislation;

[4] This case also includes several operations that are connected to each other and whose total amount exceeds the limit.

[5] Currently - 20,000 (twenty thousand) manats

6.3.3. before one-time electronic transfer of funds and one-time transactions carried out with virtual assets;

6.3.4. in case of suspicions about LP/FT or circumstances creating sufficient grounds for such suspicions;

6.3.5. in case of suspicions about the authenticity of the previously provided identification data regarding the customer or beneficial owner.

6.4. Procedures applied for establishing business relations with customers shall neither be restrictive in nature, which may result in customers refusing the Bank's services, nor include elements that limit access to the services of the Bank for the disadvantaged population.

6.5. The correctness of the information provided by a customer on the phone, e-mail and other means of communication shall be checked while establishing a business relationship.

6.6. The accuracy of the information provided to the bank shall be regularly checked at the stage of establishing business relations with new customers and during the subsequent course of operations.

6.7. The establishment or continuation of business relations with customers is refused when the following, including but not limited to, other cases determined by relevant legal acts are revealed as a result of regularly conducted investigations based on the information obtained about customers:

6.7.1. if there are reasonable suspicions about the customer's involvement in LP/FT;

6.7.2. if there are reasonable suspicions about the customer's participation in transnational organized crime, as well as in supporting armed separatism, extremism and hired work, in the illegal circulation of narcotic drugs and psychotropic substances;

6.7.3. if the financial-credit organization is not physically available in the area where it is registered;

6.7.4. if measures are not taken in full extent in the field of FLP/FT of the financial and credit institution;

6.7.5. if the necessary documents are not submitted by the customer or if false documents (data) are submitted.

7. Identification and verification measures

7.1. Customer identification and verification includes the following measures:

- standard identification and verification measures;
- simplified identification and verification measures;
- additional identification measures.

7.2. Standard identification and verification measures

7.2.1. Standard customer identification procedure is carried out on the basis of the following documents:

- for natural persons - a document confirming the identity in the manner determined by the legislation;
- for legal entities - a notarized copy of the legal entity's charter and extract from the state register of legal entities, except for the cases where it is obtained through the electronic information system of the relevant registration authorities;
- for natural persons engaged in entrepreneurial activity without creating a legal entity - a document confirming the identity in the manner determined by legislation and a certificate issued by the relevant tax authority.

7.2.2. Verification of the obtained identification data about the customer and the beneficial owner shall be carried out through reliable and independent sources[6];

7.2.3. Individual customers shall be investigated whether they act on their own behalf or on behalf of another person;

7.2.4. The legal address of the legal entity, the name of the founders, the legal status of the legal entity, the organizational-legal form and the head of the legal entity[7] shall be identified on the basis of the document on the legal entity's charter and state registration;

7.2.5. Appropriate measures are taken to determine the natural persons who are the real owners[6] of the legal entity in order to determine the beneficial owner of the customer being legal entity;

7.2.6. Verification measures are continued until the absolute certainty about the identification of the beneficial owner and the identification of his identity;

7.2.7. It is checked whether the natural person acting on behalf of the customer being legal entity is authorized in this regard and if it is determined that he is an authorized representative, an appropriate document[8] confirming it is required;

7.2.8. If business relations, financial transactions or other transactions are carried out through a legal representative, identification and verification of both the represented person[9] and the representative is carried out.

7.3 Simplified identification and verification measures

[6] Electronic databases, Internet resources and so on

[7] Executives having the right to sign first

[8] For example, power of attorney

[9] Beneficial owner

7.3.1. These measures are applied taking into account the nature of the customer, business relations and the performed operations and the risks they may cause, consisting of identification measures applied in relation to customers and transactions with low LP/FT risks;

7.3.2. Simplified identification and verification measures may be applied to business relations and transactions before the establishment of business relations and before any one-time transaction[11] expected to be carried out within the limits[10] or more than the limit established by legislation;

7.3.3. Identification and verification of the client and beneficial owner, determination of the purpose and essence of the client's business relations and regular updating of the obtained information can be carried out in a simpler and limited scope within the framework of simplified identification and verification measures;

7.3.4. Simplified identification and verification measures that can be applied to low-risk business relationships include:

- verification of the customer and the beneficial owner after the establishment of business relations[12];
- reducing the regularity of updates on customer identification;
- reducing the level of regular monitoring and examination of transactions based on the minimum threshold of the appropriate amount determined by internal bank rules;
- obtaining information about the purpose and nature of business relations from the conducted transactions and established business relations.

7.4 Additional identification measures

7.4.1. Additional identification measures are applied to persons who have large amounts of money or valuable property of unknown origin and who are classified as high-risk customers according to internal bank regulations;

[10] Currently - 20,000 (twenty thousand) manats

[11] This case also includes several operations that are connected to each other and whose total amount exceeds the limit.

[12] For example, if the transactions on the account are not above the minimum limit set by the FLP/FT Law

7.4.2 According to internal bank regulations, security measures designed to protect privacy shall not prevent the verification of information about persons belonging to the category of high-risk customers and their activities by the Bank and the person in charge of the CCS, auditors, responsible structural unit, structural units responsible for risk management and internal control in the Bank, as well as other competent structural divisions.

7.4.3 Additional identification includes the following measures:

- verification of accounts and business relations or clarification of the purpose and nature of the carried-out transaction;
- studying the shareholders and participation shares of the customer being legal entity;
- obtaining and confrontation of more accurate information about the customer, beneficial owner and the source of the property through other reliable sources (if possible).

7.4.4 Additional identification measures are implemented for the high-risk operations mentioned below, as well as during business relations with the following high-risk customer categories:

7.4.4.1 Upon operations:

- transactions with non-resident customers;
- transactions with legal entities being nominal custodians or having issued bearer shares;
- circumstances giving suspicion or sufficient grounds for such suspicion that the property has been acquired through crime or financing of terrorism;
- any transactions with property related to citizens of states (territories) on the list of high-risk zones, persons whose registration, residence or main place of activity is in that state (territory), as well as persons who have an account in a bank registered in the specified states (territories);
- transactions on receiving funds from an anonymous account or transferring funds to an anonymous account outside the jurisdiction of the Republic of Azerbaijan;
- assets of persons subject to sanctions within the framework of the fight against financing of terrorism, as well as legal entities owned or controlled by these persons, including natural and legal persons acting for or on behalf of these persons and transactions with those assets.

7.4.4.2 Upon high-risk customer categories:

- legal entities entrusted with the management of cash, securities or other property;
- political persons of influence;
- persons conducting transactions with foreign banks through correspondent accounts;
- persons conducting transactions using technological means without establishing direct contact;
- persons conducting unusual and suspect transactions.

7.4.5 The scope of political persons of influence, their close relatives and partners shall be identified, their transactions shall be monitored and suspect transactions shall be investigated when detected within the framework of additional identification measures.

8. Establishment of correspondent relations

8.1. A respondent conducting transactions through correspondent accounts of the bank shall have sufficient information about the bank to get acquainted with its business activities.

8.2. The bank shall establish correspondent relations only with foreign banks effectively supervised by the supervisory authorities in the relevant field.

8.3. A self-assessment questionnaire shall be submitted to the foreign bank and required to be filled while opening a correspondent account of a foreign bank. That questionnaire shall be evaluated by the person in charge of the bank and the results shall be reported to the accountable manager.

8.4. The decision to open a correspondent account of a foreign bank is made by the Board of Directors. Special attention is paid to the lack of correspondent accounts of the respondent bank offering services without physical presence in any country.

8.5. Correspondent relations shall not be established with shell-type companies and such relations established earlier shall not be continued.

8.6. While establishing business relations or continuing existing relations with respondent banks located in jurisdictions identified as countries not having high standards in the field of FLP/FT and are not inclined to cooperate in this field, they are guided by the followings:

8.6.1. the presence of the respondent bank's internal regulations on identification and verification is investigated;

8.6.2. additional identification measures are taken in operations carried out through correspondent accounts.

9. Remote account opening

9.1. The bank shall apply the customer identification, verification and additional identification rules and procedures applied while opening accounts for customers establishing business

relations using technological means without establishing direct contact.

9.2. Here, the services of a reliable third party can be used while performing additional identification measures. The potential risks that may arise shall be evaluated and the customer identification and verification procedures shall be constantly updated taking into account new technological means.

10. Conducting unusual operations

10.1. The purpose and nature of unusual transactions shall be clarified at a reasonable level in comparison with similar transaction models, the source of the property presented during such transactions shall be identified and an analysis report shall be drawn up.

10.2. In cases where the degree of risk on unusual transactions is high, as well as when it is determined that the risk is high based on the evaluation of criteria related to the characteristics of customers, products, services, operations, delivery channels and geographic location and based on the results of risk assessments, enhanced customer compliance measures shall be applied.

10.3. When it is determined that the risks of LP/FT are high in unusual transactions, the relevant information is submitted to the FMSRA, the auditor, the criminal prosecution authorities or the supervisory authorities, if necessary.

11. Risk management, control and monitoring

11.1. Accounts of customers and transactions carried out through them, as well as information about the purpose and nature of business relations of customers are regularly monitored by the responsible structural unit and the intensity of monitoring is increased in proportion to the increase in risk level.

11.2. Customer identification data shall be updated regularly depending on the level of risk.

11.3. When unusual transactions are carried out and it is determined that significant changes have occurred in the data previously provided by the client, the identification data of customers shall be updated.

11.4. Prohibited and restricted areas of activity are determined by the appropriate decision of the Board of Directors on the basis of a risk-based approach and updated annually in the bank.

12. Accountability

12.1. Responsible structural unit shall prepare a report on the implementation of the measures specified in this Policy and submit to the Board of Directors at least once a year. The report shall include at least the following:

- Analysis of risks in terms of the principle "Know your customer";
- measures implemented in the direction of KYC in the current year;

– planned measures in the direction of KYC for the next year(s).

12.2. The annual report resulting from the information mentioned in clause 12.1 of this Policy is submitted to the Supervisory board after approval by the Board of Directors.

13. Responsibility

13.1. All employees of the Bank are directly responsible for the proper fulfillment of the requirements of this Policy.

13.2. Person in charge of the bank is responsible for the implementation of the measures defined by the legislation on FLP/FT in the bank, conducting trainings, establishing a control and reporting system, monitoring transactions.

13.3. Violation of the requirements stipulated in this Policy (or creation of conditions for violation) may lead to the emergence of responsibility provided for in the legislation of the Republic of Azerbaijan.

14. Final conclusions

14.1. This Policy comes into force after being approved by the Supervisory board of the Bank.

14.2. Any additions and modifications to this policy may be made by the decision of the Supervisory board.