

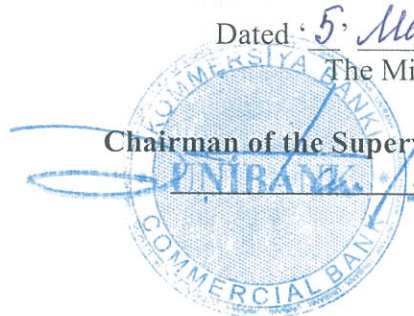
APPROVED by
The Resolution of the Supervisory Board of
“Unibank” “Commercial Bank” Open Joint-Stock Company

Dated: 5 March 2020

The Minutes No 4

Chairman of the Supervisory Board

E Garibov



THE POLICY of

“Unibank” “Commercial Bank” Open Joint-Stock Company on the Prevention of legalisation of criminally obtained funds or other property and financing of terrorism

1. The General Provisions

- 1.1. The present Policy sets the general rules of in-house rules of preventing the legalisation of criminally obtained funds or other property and financing of terrorism (ML/FT hereunder respectively) in the “Unibank” “Commercial Bank” Open Joint-Stock Company (the Bank hereunder). The principal aim of the present Policy is to exclude any ML/FT opportunity whatsoever by implementing the internal banking control.

2. The Purpose of the Policy

- 2.1. Legalisation (laundering) of funds derived from terrorism, drug business, illegal arms trade, corruption, human trade, etc) has taken on a large scale over the few decades past. That necessitated the uniting of the international community efforts to counter this negative phenomenon of the modern age that has become especially acute against the background of the national and international terrorism;
- 2.2. To avert the threat of the intervention of criminally gained capitals in their national economies and to counter the spread of terrorism, the states are combatting the ML/FT activities. Banks and other finance institutions are amongst the most suitable and opportune means of restricting and averting ML/FT encroachments attempted by criminals. Meanwhile, the growing integration of finance markets and the free capital flows between them have become a notable facilitator of the intervention of criminal-gained capitals in finance markets with the subsequent legalisation of such capitals and their exportation from a given national market;
- 2.3. The Bank is one of the banks implementing the internal control procedures with the purpose of countering ML/FT and contributing to a healthy economy growth. The Bank and its branches fully realise the necessity of protection against all attempts at abusing it as a means of legalising criminal proceeds, be it financial or other assets;
- 2.4. The Bank has built its AML/CFT action on the basis of the principles that satisfy the recommendations of the Financial Action Task Force (FATF), the European Union’s Committee

of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism(Moneyval), the Basel Committee on Banking Supervision (BCBS), the General AML/CFT Directives for the Private Banking Sector (the Wolfsberg Principles), the Law of the Azerbaijan Republic 'On the Prevention of the Legalisation of Criminally obtained funds or other property and the Financing of Terrorism' ('the Law' hereunder) and the pertaining legislation that regulate the relevant legal relations. The Bank is governed by the Know Your Customer principle, which, in turn, provides for advance identification of suspicious acts by customers. Thus, the Bank ensures the constant updating of the customer information, document accounting and registration and identification, verification and additional identification of each new customer and beneficiary in line with the Know Your Customer orientation. The present Policy is aimed at increasing the probability of compliance with the universally accepted approaches to banking;

- 2.5. The Bank strives to reduce the probability of its customers becoming victims of ML/FT and other related illegal, criminal and undesirable activities and transactions;
- 2.6. The Bank identifies and verifies customers and beneficial owners relying on the current legislation of the Azerbaijan Republic and prevents possible adverse developments (criminal acts). For instance, anonymous accounts, deposits and deposit certificate issues are not allowed; neither are allowed suspicious transactions with enterprises situated in offshore areas and with shell-banks; such events are averted as well. At the same time, acting on the basis of the aforementioned laws, the Bank establishes its in-house procedures and rules, and prevents illegal acts from emerging. The Policy of the Bank is based on the clear definition of the general approaches held by the Administration and on the exacting distribution of responsibilities. The Policy is applied not only to the Head Office of the Bank but also to all its sub-divisions and branches, and is devised to ensure and maintain the following:
 - Minimisation of the risks of the Bank being abused as an ML/FT transaction intermediary;
 - Protection of the Bank against image and operating risks stemming from it being abused for ML/FT transactions;
 - Services are provided and banking operations are conducted only as instructed by the customers of integrity;
 - Identification of transactions subject to mandatory control and of suspicious transactions; registration and communication of information about such transactions to the concerned authorities;
 - Presentation of documentary argumentation by the Bank in the course of investigations into possible ML/FT affiliations of a customer of the Bank.

3. The Internal AML/CFT System

- 3.1. The AML/CFT System of the Bank consists of the following elements:
 - The Policy, the in-house regulations and procedures;
 - The compliance officer ;
 - The AML/CFT training process;
 - Internal Audit.
- 3.2. The Bank develops and applies appropriate internal control measures and a realisation programme for them in order to maintain efficient operations of its AML/CFT system; this overall process incorporates the following elements:
 - The procedures for identification and verification of the customers and beneficial owners of the Bank;

-
- The criteria (indicators) of transactions subject to monitoring;
 - The rules of identifying and preventing transactions that are suspicious by the in-house corporate regulations and of reporting relevant information to the Financial Monitoring Service;
 - It being in keeping with the in-house corporate regulations, the Bank's cash transactions with money or other funds worth AZN 20,000 or more are classified as current transactions and the rules in place require that the Financial Monitoring Service should be notified of same;
 - The information documenting and confidentiality provision rules;
 - The rules of employment and of employee checking;
 - Compliance with the principles of making business lawfully and in good faith.
- 3.3. The in-house control procedures in use make it possible to assess the AML/CFT risks;
- 3.4. Pursuant to Item 9.13 of the Law, the Bank shall assess the ML/FT risks related to the specific features of a customer and in so doing shall consider such factors as a customer's occupation, the kind of the operation and its frequency. The Bank shall regard the following customers as the high-risk ones:
- Politically exposed persons of foreign country. By 'politically exposed persons of foreign country' we mean the persons listed in Item 1.0.14 of the Law:
 - In order to establish whether a person is apolitically exposed persons of foreign country, every new customer must supply the relevant information; besides, such kind of information must be verified with reliance upon open sources and special digital data bases. A foreign national may be requested to fill in a form (a questionnaire) designed to establish whether he/she is apolitically exposed persons of foreign country;
 - The Bank must regularly control its current business relations with politically exposed persons of foreign country and take steps to ensure periodical updates in the identification and verification documentation on them;
 - In keeping with Item 9.13 of the Law, the Bank must apply additional identification measures to the politically exposed persons of foreign country and other high-risk customers.
 - Non-resident customers;
 - The corporate entities in charge of money, securities or other property;
 - The corporate entities that are nominal holders or issuers of documentary bearer shares;
 - The persons in the approved lists of the Financial Monitoring Service;
 - Citizens of the states (territories) in the approved list of the Financial Monitoring Service; also, persons whose places of registration, abode and main places of business are such states (territories) as well as persons who maintain accounts with the banks registered in such states (territories);
- 3.5. The following measures are taken with regards to ML/FT:
- Timely identification, registration and communication to an authorised AML/CFT action body of information about transactions subject to mandatory control and about suspicious transactions;
 - Declination of a transaction if it is known that at least one of the transacting parties is engaged in terrorist activities and refusal to open and maintain an account or conduct a transaction if the requesting customer fails to submit the required information or submits false information as well as where it is known that an individual or legal entity is engaged in terrorist activities;
 - Registration and storage of information;

-
- Training of the Bank's staff and improvement of their professionalism.
- 3.6. The Bank shall, for the duration of the periods specified below, store on either data carriers or electronically the identification documents referenced in Article 9 of the Law and documents regarding transactions with funds or other property as well as documents about the transactions referenced in Articles 9.1 and 9.2 of the Law:
- All the information and documents obtained in the course of the identification and verification of a customer, a beneficiary owner or an authorised representative; business correspondence and other account-opening documentation – for at least five years upon closure of the customer account or termination of legal relations with the customer;
 - Information and documents about a customer's operations with funds or other property conducted in the country or internationally, where such information and documents permit recovery of a transaction inclusive of its amount and currency – for at least five years upon completion of such an operation;
 - With the inclusion of the findings of an analytical study undertaken to identify the purpose and essence of unusual transactions, all the documents and information about the transactions covered in Article 9.2 – for at least five years upon cessation of legal relations with the customer.
- 3.7. The Policy contemplates training the employees in the skills required to counter the legalisation of criminally obtained funds and the finance of terrorism as well as to abide by the internal control system development requirements and follow the AML/CFT laws, the in-house corporate acts and corporate control system, the relevant implementation programmes and internal controlling procedures. The education and training are mainly conducted with the following persons and must be made applicable not only to the Head Office but also to each Branch of the Bank:
- The Compliance officer;
 - The legal and internal audit department staff or other employees who discharge the relevant functions;
 - The front-office employees, group leaders and heads of the relevant subdivisions of the Bank;
 - In consideration of the structure and operating specificities of the Bank, also the other employees engaged in operational management and decision-making in the Bank.
- 3.8. The education and training are undertaken once a year, in case of material amendments to a law or the internal corporate acts, etc;
- 3.9. The Bank shall define the maintenance of the functioning AML/CFT counter systems, the control over the co-ordination of the operations of the subdivisions of the Bank and their observance of the relevant internal control rules and programmes as well as the communication to the appropriate authorities of the information about operations subject to mandatory control and about suspicious operations and, last but not least, the Compliance officer reporting the information on counter effect on AML/CFT information to the appropriate authority. At the same time, and in order to ensure the efficient AML/CFT action to avert possible illegal occurrences, the Bank shall use the Compliance officers who are the persons in possession of the relevant knowledge and literacy. All hard-copy and digital forms and documents relevant to that activity shall be archived in hard copy and digitally for at least 5 years upon the closure of a customer account or cessation of the legal relations with a customer, and shall be made available to the appropriate authority if need be;
- 3.10. **The Compliance officer** shall be a natural person responsible for controlling the implementation of the AML/CFT rules and procedures at the administrative levels of the Management Board and the Supervisory Board as well as at those of the management bodies of the sub-divisions of the

Bank, Compliance officer exchanging the information with the Financial Monitoring Service and the reporting on operations subject to mandatory control. Employing and discharging the Compliance officer shall be subject to appropriate decisions of the Management Board. The following experience and professionalism requirements put to the Compliance officer shall be satisfied at all times:

- 3.10.1. University education and at least 2 years of practical employment experience within the main operating field of the monitoring subject;
- 3.10.2. Knowledge of the national legislation as well as the international standards and requirements in the AML/CFT field;
- 3.10.3. Awareness of the principal individual operating areas of the monitoring subject;
- 3.10.4. Proficiency in the Azerbaijani language;
- 3.10.5. No previous criminal records.
- 3.11. The following persons may not be the Compliance officer:
 - 3.11.1. Those employed by another monitoring subject;
 - 3.11.2. Those in close blood relation to members of the administration/management team of the monitoring subject.
- 3.12. For the purposes of Item 3.11.2. of the present Policy, the wording 'close blood relation' shall denote a spouse, parents, children, stepparents, stepchildren, siblings, parents-in-law or siblings of all the previous relatives;
- 3.13. A Compliance officer of an entity within the monitoring subject shall be appointed by the appropriate decision (order, decree, etc) specifying the information proving this person's compliance with the requirements contained in Item 3.10 of the present Policy. One counterpart of the decision signed by the administration of the monitoring subject shall be submitted to the Financial Monitoring Service within 2 (two) business days;
- 3.14. The Bank has the internal audit mechanism checking for efficiency the application of the legal and regulatory AML/CFT requirements as well as that of the existing internal-control regulations and procedures. The goal of the Internal Audit, which is one of the components of the AML/CFT programme of the Bank, is to make the Supervisory Board of the Bank reasonably certain that the present Policy is satisfactory and sufficient for the purpose. The Internal Audit undertakes the annual risk-based assessment of the Policy governance, the adherence to the rules, the risks, the sufficiency and efficiency of the controlling and training activities, the effectiveness of the Policy and the compliance of the current operations with the requirements contained in the national legislation;
- 3.15. The AML/CFT Unit of the Bank only reports to the Chairman of the Management Board while the AML/CFT Compliance officer only reports to the Chairman of the Supervisory Board and the Chairman of the Management Board of the Bank. Such reports must be submitted to the Chairman of the Supervisory Board every six months and to the Chairman of the Management Board on the monthly basis;
- 3.16. It is permissible to conduct transactions with the states (territories) determined by the Financial Monitoring Service ('The Black List of Countries') with which it is not mandatory to disclose identification information in financial operations over suspicions of supporting ML/FT, transnational organised crime, armed separatism, extremism and mercenary activists, illicit traffic in narcotics or psychotropic drugs and/or with the customers classified as high-risk persons once there are relevant affirmatory opinion statements by the AML/CFT Unit of the Bank and the Compliance officer alike;

-
- 3.17. Under no circumstances shall the Bank conduct transactions with customers having Armenian surnames (and being of Armenian descent);
 - 3.18. Should a customer decline to submit the required identification information by means of the appropriate AML/KYC (anti-money laundering/know your customer) questionnaire forms or where it has been established that the identification information a customer has provided earlier is untrue, the Bank will not build business relations with, and will not open a bank account for such a customer;
 - 3.19. The present Policy is based on the Law, the regulations and indicators determined by the Financial Monitoring Service, regulatory legal acts and the recommendations of the Financial Action Task Force (FATF), the European Union's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism(Moneyval), the Basel Committee on Banking Supervision (BCBS), Wolfsberg principle, as well as the legal documents enacted with reliance upon the international and domestic legislations.

4. Effectiveness of the Policy

- 4.1. The present Policy shall become effective as of its adoption date and shall hold effective for the duration of one year. The present Policy shall be reviewed at least once a year and amended as necessary pursuant to the relevant decisions of the Supervisory Board of the Bank;
- 4.2. The former pertaining Policy, the addenda and amendments thereto shall be deemed null and void as of the date of adoption and announcement of the present Policy.