Translated from Russian into English

"APPROVED"
by the decision of the Council of "Kapitalbank" JSCB
Minutes № 54 as of December 25, 2019
Chairman of the Council of the bank
Abdusamadov M.A.
signature

Official stamp:
Republic of Uzbekistan, Tashkent city
Joint-stock commercial bank "Kapitalbank"

POLICY
ON COUNTERING MONEY LAUNDERING AND TERRORISM FINANCING OR FINANCING OF THE PROLIFERATION OF MASS DESTRUCTION WEAPONS AT "KAPITALBANK" JSCB (NEW WORDING)

Tashkent – 2019

BACKGROUND

Taking into consideration significance and particular importance of the anti-money laundering policies implemented throughout the entire civilized world, including the threat posed to the entire world community from terrorist and other related organizations, as well as to prevent the threat of money laundering and efficient identification and suppression operations aimed at the legalization of money laundering, prevention of intentional or unintentional involvement of the bank in the criminal activity and ensuring strict Compliance with the requirements of the legislation on countering money laundering and terrorism financing at "Kapitalbank" JSCB (hereinafter referred to as the bank) there has developed and implemented in practice a set of measures aimed at urgent detection of doubtful and suspicious transactions.

The bank undertakes all possible measures to prevent operations and transactions that are directly or indirectly related to the money laundering, as well as to exclude the possibility of making operations related to the financing of terrorist activities or financing the proliferation of mass destruction weapons.

The bank carefully approaches selection and formation of its customer base on the principle of "Know Your Customer", thoroughly examines its customers, interests and areas of their activities and seeks to establish relationships based on transparency and understanding of customers' business activities and operations.

Chapter 1. GENERAL PROVISIONS

1. This Policy on countering money laundering, terrorism financing, or financing of the proliferation of the mass destruction weapons at "Kapitalbank" JSCB (hereinafter referred to as the "Policy" has been developed in compliance with the laws of the Republic of Uzbekistan "On banks and banking activities" (new wording) "On bank secrecy", "On counteracting money laundering and terrorism financing", as well as the Internal Control Rules on countering money laundering and terrorism financing at commercial banks, approved by a joint resolution of the Executive Board of the Central Bank of the Republic of Uzbekistan № 343-B on April 17, 2017 and the Department Agency for Combating Tax, Currency Crimes and Money Laundering under the Prosecutor General's Office № 14, registered by the Ministry of Justice of the Republic of Uzbekistan under № 2886 on May 23, 2017, the Regulation on the minimum requirements for the activities of commercial banks in their relations with consumers of banking services registered by the Ministry of Justice of the Republic of Uzbekistan under № 3030 on July 2, 2018, as well as the recommendations of the Group (intergovernmental commission) on the development of financial measures on countering money laundering (FATF).

2. The procedures and rules specified in this Policy are subject to amendments and additions, in compliance with changes in the legislative framework of the Republic of Uzbekistan and international norms and standards.

3. The following basic concept are used in this Policy:

FATF is the Intergovernmental Commission against money laundering, which develops global standards in the field of countering money laundering and terrorism financing, as well as assesses the compliance of the national systems for countering money laundering and terrorism financing with these standards;

Money laundering - a criminally punishable socially dangerous act, which represents shaping in the legal form of the origin of ownership (cash or other property) by transfer, conversion or exchange, as well as concealment or hiding of the true nature, source, location, method of disposal, movement, undoubted rights in relation to money or other property or its property, if money or other property is obtained as a result of criminal activity;

terrorism financing - a criminally punishable socially dangerous act aimed at ensuring existence, functioning financing of a terrorist organization, leaving abroad or moving along the territory of the Republic of Uzbekistan for participating in terrorist activities, preparation and commission of terrorist acts, direct or indirect provision or collection of any facilities, resources, other services to terrorist organizations or to persons assisting or participating in terrorist activities;

financing of the proliferation of the mass destruction weapons - provision or collection of any facilities, resources, other services for the development, production, acquisition, stockpiling,

storage, marketing, use of nuclear, chemical, biological and other types of mass destruction weapons, materials and equipment that may obviously be used in its creation;

list - a list of persons participating in or suspected of participating in terrorist activities or the proliferation of mass destruction weapons, compiled by a duly authorized public body on the basis of information provided by public authorities engaged in the fight against terrorism and the proliferation of mass destruction weapons, and other competent authorities of the Republic of Uzbekistan, as well as the information received through official channels from the competent authorities of foreign states and international agencies.

risk - the risk of customers to make transactions with the aim of money laundering or terrorism financing;

department of the internal control of the bank – a structural subdivision of the bank responsible for internal control in order to counter money laundering and terrorism financing;

responsible employee - a bank employee responsible for compliance by the bank with the rules of internal control in order to counter money laundering and terrorism financing and providing the information to a duly authorized public body;

customer - an individual/legal entity/individual entrepreneur intending to initiate business relations with the bank, or already being serviced by the bank, or making a one-time transaction with the bank on his own behalf, or in favor of third parties;

transaction participants are customers, their representatives, as well as partners/counterparties of the customer participating in the transaction;

third party – agencies engaged in transactions with cash or other property;

beneficiary owner - a person who ultimately owns property rights or actually controls the customer, and in whose favor a transaction with cash or other property is made;

identification of the beneficial owner of the customer - the bank determines the legal entity of the owner, including the person of the controlling customer by examining the ownership and management structure on the basis of constituent documents determined by law (charter and (or) constituent agreement, regulation);

public officials are persons appointed or elected permanently, temporarily or by special authority, performing organizational and administrative functions in public authorities and authorized to perform legally significant actions, as well as persons performing these functions an international agency, either in the legislative, executive, administrative, or judicial body of a foreign state;

close relatives - parents, blood and step brothers and sisters, spouses, children, including adopted children, grandfathers, grandmothers, grandchildren, as well as parents, blood and step brothers and sisters of spouses;

duly authorized public body (hereinafter referred to as the "DAPB") - the Department for countering economic crimes under the Prosecutor General's Office of the Republic of Uzbekistan;

branches - branches, banking services centers, Operational Board, call centres of "Kapitalbank" JSCB.

Chapter 2. BASIC PRINCIPLES

4. With the aim of preventing the involvement of the bank in transactions related to the money laundering and terrorism financing or the financing of the proliferation of mass destruction weapons, the bank is guided by the following basic principles:

follow general approaches set forth in this policy when creating and improving the internal control system in order to counter money laundering and terrorism financing;

develop their own internal control rules in order to counter money laundering and terrorism financing or the financing of the proliferation of mass destruction weapons based on the national legislation and this policy;

undertake actions aimed at identifying, assessing and mitigating risks associated with involving the bank in money laundering or terrorist financing schemes during all banking transaction, including currency transactions, bringing bank services to customers, establishing

correspondent relationships, as well as introducing new technologies, etc.

Chapter 3. BASIC OBJECTIVES

5. The basic objectives in countering money laundering and terrorism financing are the following:

a) arranging an efficient system of internal control to identify transactions to be reported to the DAPB in all structural subdivisions and branches of the bank;

b) efficient identification and suppression of transactions with money or other: property aimed at money laundering and terrorism financing or the financing of the proliferation of mass destruction weapons;

c) preventing intentional or unintentional involvement of the bank in criminal activity, penetration of criminal capital into its charter fund (capital), as well as the penetration of criminals into the management of the bank;

d) ensuring strict compliance with the requirements of the law on money laundering and terrorism financing or the financing of the proliferation of mass destruction weapons;

e) study of the internal control system of other banks of the Republic of Uzbekistan and foreign banks in the establishment of correspondent relations thereto.

Chapter 4. RESPONSIBLE EMPLOYEE OF THE BANK

6. Taking into consideration that the bank performs various types of transactions (settlement, cash, deposit, currency, credit operations, etc.), the implementation of this policy is the responsibility of the heads of structural subdivisions and the management of branches directly involved in these processes, and overall supervision and control is executed by a responsible employee (who is the director of the internal control department, which manages the activities of assigned employees to branches), appointed by order of the chairman of the Executive Board of the bank.

7. A responsible employee of the bank occupies the position of the Internal Control Department, which is independent in making decisions and performing its duties.

8. A responsible employee must be adequately authoritative, amiable, honest and fair.

9. The duties of the responsible employee include the following:

ensuring the awareness of other employees of the bank on the policy to counter money laundering;

carrying out inspections for the implementation of the procedures provided for in the rules to counter money laundering and terrorism financing in the bank and monitor the elimination of violations;

'keeping records, archiving and maintaining relevant information and documentation regarding transactions affected by the rules on countering money laundering and terrorism financing or financing the proliferation of mass destruction weapons;

undertaking efficient measures on the basis of the criteria provided for by the internal rules on money laundering and terrorism financing in cases of suspicious transactions;

in compliance with the requirements of the laws of the Republic of Uzbekistan, establishing contacts with relevant authorities to comply with the implementation of legislation to counter money laundering and terrorism financing.

Chapter 5. IDENTIFICATION PROCEDURES

10. The main way to efficiently prevent money laundering is customer due diligence. Due diligence is carried out on the basis of information and documents provided by the bank customers.

11. The bank undertakes relevant measures on customer due diligence on its own in the following cases:

a) when establishing economic and civil law relations, including: when a client requests to open a bank account (deposit), unless the bank has the opportunity to conduct a customer due diligence in reliance upon previously submitted documents that are valid and verified at the date of verification;

when an individual applies for a bank card; when legal persons and (or) individuals apply with an application for the purchase of securities issued by the bank;

when legal and (or) individuals own shares in a bank in the amount equal to or exceeding one percent of its Charter capital;

when an individual applies for a loan and/or a safe custody service in a bank deposit box;

b) when performing one-time transactions in the following cases:

sale of cash foreign exchange in the amount equal to or higher than 500-fold the basic calculation value by individuals;

exchange, replacement and (or) exchange for another foreign exchange (conversion) by individuals of cash foreign exchange in the amount equal to or higher than 500-fold the basic calculation value;

receiving from customers for collection and (or) for the examination of cash foreign exchange in the amount equal to or higher than 500-fold the basic calculation value;

transactions performed by individuals with the use of plastic cards (cash withdrawal, payment for goods and services) through terminals located at a bank (except for payments for public utilities, communication services, payments to the budget, extrabudgetary funds and other compulsory payments) in the amount equal to or exceeding 300-fold the basic calculation value;

receiving from the cashier's cash foreign exchange by customers with the use of plastic cards issued by other banks for the amount equal to or higher than 100-fold the basic calculation value;

purchase by individuals of the coins of the Republic of Uzbekistan from precious metals in the amount equal or exceeding 500-fold the basic calculation value;

purchase of foreign exchange by individuals (when purchasing by the individual-resident of the foreign exchange in cash in the amount exceeding 100 USD in the equivalent);

making or receiving a money transfer without opening or using a bank account (except for payment for public utilities, communication services, payments to the budget, extra-budgetary funds and other compulsory payments);

c) when making suspicious transactions;

d) if there are doubts about the reliability or adequacy of previously obtained data about the customer.

12. Measures on the customer due diligence include the following:

a) verification of the identity and authority of the customer and the persons on whose behalf he acts on the basis of relevant documents;

b) identification of the beneficial owner of the customer;

c) a study of the aim and nature of the business relationship or planned transactions;

d) on the constant basis performing the study of business relations and transactions carried out by the customer in order to verify their compliance with the information about such a customer and its activities.

In addition to applying the above-stated measures for customer due diligence, in relation to public officials acting as the customer or the beneficial owner of the customer, the bank must:

apply reasonable measures to verify information on the status of a public official and determine the source of funds or other property for the transaction;

establish business relations with a public official only with the permission of the chairman of the Executive Board of the bank or his duly authorized deputy;

implement continuous comprehensive monitoring of business relations.

13. The bank can trust the results of the due diligence of the client conducted by third parties, according to the due diligence measures specified in clauses a) and c) of paragraph 12 of this

Policy. In such cases, the ultimate responsibility for the customer due diligence belongs to the bank itself. In this case, the bank must make assure itself:

in the possibility of immediate receipt (through electronic systems) of the necessary information on the customer due diligence;

if possible, upon request, immediate receiving copies of identification data and other relevant documents on customer due diligence;

that third parties are guided by internal rules to counter money laundering, terrorism financing and financing of the proliferation of mass destruction weapons.

In case of non-compliance with one of the requirements provided for in clause two - four of this paragraph, the bank shall undertake relevant measures for customer due diligence by its own.

The bank decides to enter into business relations with the customer by its own, in reliance upon the risk, and also has the right to undertake measures for due diligence.

Commercial banks should stipulate the possibility of undertaking measures on customer due diligence in the contract and (or) in the offer contract.

14. All documents enabling to identify the customer and other participants of transactions must be valid at the submission date. Documents compiled in a foreign language (in full, or in any part) are submitted to the bank with a translation certified according to the established procedure into the state or Russian language, and, if necessary, notarized.

15. The bank, if there is suspicion of the reliability of the information and documents received, must undertake measures to verify this information and these documents. In this case, the bank has the right to apply to the relevant agencies with a request to ascertain the reliability (authenticity) of information and documents about customers. Moreover, the bank has the right to require the submission of original documents for review, in case of doubt on the reliability of the submitted copies of documents.

16. The bank has the right to refuse the customer to make transactions with cash or other property in case of:

absence at its location (mailing address) of the governing body of a legal entity or a person authorized to act on behalf of a legal entity without a power of attorney;

submission of intentionally false documents or failure to submit the documents requested in compliance with the law.

17. The bank is forbidden:

open accounts (deposits) to anonymous owners, that is, without providing the person or legal entity opening the account (deposit) documents required for his identification;

open accounts for fictitious names that are not confirmed by documents;

open accounts without personal presence of the person opening the account or its authorized representative, unless the bank is able to identify the customer based on previously submitted documents valid and verified at the date of identification, as well as measures for the proper verification of customers have been carried out by the registering authority or the bank on the basis of biometric data, and also trusts the results of the customer due diligence performed by the third party;

establish and continue relations with non-resident banks that do not have a physical presence and permanent governing bodies within the territories of the states in which they are incorporated;

issue of securities and other bearer financial instruments;

render services for receiving and sending funds in foreign exchange, including through international money transfer systems, without identifying the customer;

establish subsidiary banks, branches or representative offices within the territory of states that are not involved in international cooperation in the field of countering money laundering and terrorism financing or financing of the proliferation of mass destruction weapons.

18. When it is impossible to perform a customer due diligence, the bank should consider sending a message to the DAPB and refuse to enter into business relations or make transaction with cash or other property of such a customer, or should terminate any business relations therewith.

§ 1. Individuals

19. The bank must have adequate evidence of customer identity. Documentary verification of the identity is implemented only in reliance upon the documents which, in compliance with the legislation of the Republic of Uzbekistan, are considered to be identity documents (passport or a substitutional document), or the biometric data.

20. When identifying an individual, the bank must identify his full last name, first name and patronymic, date and place of birth, citizenship, place of permanent and (or) temporary residence, details of the passport or a substitutional document (series and number of the document, date of issue of the document, name the authority that issued the document), a taxpayer identification number (if available) and the phone number (home/mobile - if available), as well as the biometric data.

21. Information on the customer must be confirmed by an identification document proving identity (passport or a substitutional document).

Official document:

must contain the series and number, the date of issue of the document, the name of the authority issuing the document, a photo of the customer and other information with the aim of confirming its legality;

validity period of the identification document must be effective at the time of opening the account and making transactions on the account.

opening and closing of accounts is not allowed without the presence of the account holder or his authorized representative.

In reliance upon the biometric data, it is necessary to verify such data with the information system of the Ministry of Internal Affairs of the Republic of Uzbekistan.

22. Identification documents (passport or a substitutional document) must be submitted in originals and the bank is obliged to make their copies and store them in the appropriate files.

§ 2. Legal entities and individual entrepreneurs

23. The bank undertakes all the measures required to obtain a comprehensive view of the customer, its structure, beneficial owner, and also receives additional information on the customer's core business and the reasons for his interest in a particular banking product.

24. In relation to a legal entity the bank shall identify the company name, location (mailing address), as well as information on the identification of an individual acting on behalf of the legal entity in transactions with cash or other property. Identification of a legal entity is implemented on the basis of documents provided for opening an account (including via a single window) and other documents required in compliance with the law. In the implementation of customer due diligence measures regarding legal entities, the bank should receive relevant documents on the state registration, information about managers, as well as information specified in the constituent documents.

25. If a customer or a beneficial owner is represented by a legal entity that is subject to the requirements of statutory legal acts on disclosing information on the ownership structure, then it is not required to ascertain and confirm the identity of the founders (shareholders) of such a legal entity.

26. With the aim of more comprehensive examination of the customer - legal entity in the process of due diligence, the bank should undertake reasonable and affordable measures to identify the individual - the beneficial owner, who ultimately is the owner or controls the customer, including by examining the ownership structure and management of the customer, as well as the founders (shareholders who own at least ten percent of the company's shares, participants) of the customer.

The bank should pay a particular attention to:

Composition of the founders of the customer, determination of persons owning a share of over 10% of the charter fund (capital) of the customer;

structure of customer's governing bodies and their powers;

the amount of the registered charter fund capital (capital) of the customer.

27. In the case of legal entities and individual entrepreneurs founded by residents of the Republic of Uzbekistan applying for a distant opening of a bank account in the process of the state registration, there must be undertaken the measures aimed at due verification of the customer, provided for in paragraph 26 of this Policy. These measures can be carried out by the Centers of public services (hereinafter referred to as the registration authority) and commercial banks can trust the results of the measures undertaken. In this case, the bank must assure itself:

in the ability to immediately obtain required information on measures to properly verify the customer through an automated system of the state registration and registration of entrepreneurship entities;

in compliance with the requirements for the implementation of customer due diligence measures established in legislative acts by the registration authority.

In case of failure to comply with the requirements specified in clauses two and three of this paragraph, commercial banks undertake measures on customer due diligence by its own.

When undertaking measures on customer due diligence by the registration authority, the bank makes the decision to enter into business relations with the customer by its own based on the risk. Herewith, the offer of a bank account agreement should indicate the possibility of undertaking measures on customer due diligence.

28. When identifying legal entities, the bank must also obtain the information on the persons who manage the activities of the legal entity, working in its executive bodies, and have the right to dispose of its assets and liabilities. Meanwhile, with regard to legal entities, it is required to verify the company name of the agency, as well as the officials whose data are contained in the card with samples of signatures and seal imprint, with the List.

29. Customer due diligence measures are not required for public administration authorities.

30. The information required for the identification of individual entrepreneurs is as follows:

a) information provided for the identification of individuals;

b) information on the state registration: date, number, name of the registration authority;

c) the place of doing business;

d) other data specified in the certificate of the state registration:

e) information on the available certificates and licenses for doing any type of business: type of business, number, date of issue: by whom it was issued; validity;

e) phone numbers.

§ 3. Public officials

31. One of the main tasks of the bank's internal control system is to perform a comprehensive monitoring of transactions made by public officials and their close relatives;

32. In addition to applying the customer due diligence measures referred to in this Policy in relation to the public officials acting as the customer or a beneficial owner of the customer, the bank shall:

apply reasonable measures to verify information on the status of a public official and determine the source of funds or other property on the transaction;

establish business relations with a public official only with the permission of the Chairman of the Executive Board of the bank or his authorized deputy;

perform continuous comprehensive monitoring of business relations.

33. Public officials and members of their families are also referred to high-risk category and the bank should pay a particular attention thereto.

§ 4. Associations and charity funds

34. In case the accounts are opened for association and charity funds, the bank must verify the legitimacy of the goals of establishing these entities. The bank must receive all legal documentation of such entities (including from a single window), personal information about the beneficial owner and the persons authorized to manage the accounts. This data should be constantly updated as the structure of the entity and authorized persons change.

§ 5. Credit institutions

35. When establishing business relations with a credit institution, regardless of the level of

these relations, it is necessary to obtain and study constituent documents, state registration documents and other documents submitted (including through a single window) for establishing business relations for identification purposes. Moreover, it is required to find out what measures to counter money laundering and terrorism financing are undertaken by this credit institution.

36. When establishing and implementing correspondent relations with a non-resident bank, in addition to identifying this institution, the bank:

gathers the information about a non-resident bank adequate to get a comprehensive view of the nature of its business activities:

on the basis of open information determines the reputation and quality of supervision, including whether there have been investigations in relation to this bank regarding the money laundering and terrorism financing;

in relation to "transit accounts" it should receive reasonable confirmation that the correspondent bank has established an identity and verifies customers who have direct access to the correspondent's accounts and that he is able to provide required identification information about the customer at the request of the correspondent bank;

with the aim of making transit transfers, keep all information about electronic transfers when establishing relations with other banks.

The decision to establish correspondent relations with a non-resident bank is made by the Executive Board of the bank.

37. The bank should pay particular attention to the continuation of correspondent relations with non-resident banks located within the territory of states that are not involved in international cooperation in the field of countering money laundering and terrorism financing, or by their subsidiary banks, branches and representative offices.

The bank needs to assure itself that non-resident banks, which correspondent relations are established with, apply international verification standards and use appropriate verification procedures for transactions.

38. The bank is obliged to undertake measures aimed at preventing the establishment of relations with non-resident banks, for which there is information that their accounts are used by banks that do not have permanent governing bodies within the territories of the states in which they are incorporated.

39. When making international settlements, the bank may transfer payment details and other information related to the settlements, specified above, to the correspondent banks.

40. If there is some information about a violation by a non-resident bank of the requirements of international standards for countering money laundering and terrorism financing or financing of the proliferation of mass destruction weapons, the Executive Board of the bank should consider undertaking appropriate measures even to the extent of termination of cooperating with this correspondent bank.

§ 6. International money transfer.

41. When establishing and implementing relations with companies rendering services for international money transfers, in addition to identifying the institution, the bank:

gathers the information about a partner on international money transfers in order to get a comprehensive view of the nature of his business activities;

on the basis of open information determines the reputation, including whether investigations of violations related to money laundering and terrorism financing, or financing of the proliferation of mass destruction weapons have been made with respect to this institution;

stores all information about e-transfer.

42. The decision to establish relations with international money transfer systems is made by the Executive Board of the bank.

43. When making transactions on international money transfers, including through international money transfer systems, the bank must:

make money transfer transactions after customer due diligence of customers - individuals;

provide forwarding of sent money transfers with accurate information about the sender;

require non-resident banks and international money transfer systems to provide minimum information about the senders of funds in compliance with the requirements of national legislation and internal local documents of the bank;

undertake reasonable and affordable measures to identify international money transfers that do not have the required information about the recipient and (or) the sender on the basis of the Procedure for implementing measures at "Kapitalbank" JSCB in cases of the identification of international money transfers that do not have the required information about the recipient and (or) about the sender approved by the Executive Board of "Kapitalbank" JSCB;

pay a particular attention and perform a comprehensive analysis of transactions related to international money transfers in which information about the sender (last name, first name, patronymic of individuals, full name of legal entities, address and account number of the sender) is not presented or is not presented in full.

44. The bank must be able to obtain additional information about the senders of funds from correspondents of non-resident banks and international money transfer systems in compliance with the agreements compiled therein within 3 (three) banking days.

45. In case of absence of such possibility, it is required to consider the termination of the contract with such systems of international money transfers by the decision made by the Executive Board of the bank.

46. If a bank acts as an intermediary (transit bank) in a payment transfer, then it must:

ensure the transfer and storage of all information about the sender and receiver accompanying the electronic transfer, together with the transfer for at least 5-year period;

undertake reasonable and affordable measures to identify international money transfers that do not have the required information about the recipient and (or) the sender;

consider sending a message to the Department in case of revealing international money transfers that do not have the required information about the recipient and (or) the sender.

§ 7. Currency transactions

47. The bank interacts with the Central Bank on the issue of providing the bank with a software package of a "unified system of currency exchange offices" for registering transactions on the purchase and sale of foreign exchange with an automated banking system.

48. The bank installs the ATMs to provide services for withdrawing foreign currency in cash purchased by individuals from international payment cards (conversion cards), and also provides services for accepting deposits in foreign currency.

§ 8. Rendering banking services to customers

49. The bank provides customers with complete information about the services rendered by the bank, including through the placement of this information on the bank's website and information stands of the bank branches.

50. On its own website the bank publishes training programs in the form of lectures and videos on the services and products of the bank and a mechanism for obtaining certain types of banking services, as well as information on improving financial literacy.

51. Develops and manufactures necessary handouts for banking services (tariffs, flyers, booklets).

§ 9. New technologies

52. The bank develops the program to provide distant banking services (Internet banking, mobile banking).

53. Development of a mechanism for receiving and processing customer payment documents, as well as monitoring the status of payments and customer accounts around-the-clock through distant banking servicing.

54. The bank should undertake measures to prevent the abuse of technological advances with the aim of money laundering and terrorism financing or to finance the proliferation of mass destruction weapons. For these purposes, the bank must determine and evaluate the levels of risk

that may arise in connection with:

with the development of new types of services and new business practices;

using new or developing technologies for both new and current types of services.

55. Such a risk assessment should be performed before launching new types of services, business practices or using new or developing technologies. Therein, time, determination and assessment of this risk should be implemented by the bank's subdivision directly introducing new types of services (new technology), in cooperation with the Internal Control Department.

This subdivision of the bank and the Internal Control Department should undertake appropriate measures to monitor and reduce these risks.

Information on the results of measures undertaken should be provided to the Executive Board of the bank.

§ 10. Update of the customer data

56. The Bank takes steps to properly update customer information obtained as a result of customer due diligence and identification. In order to keep customer information up to date, the bank updates its customer information at least once every three years. The review and updating of information about high-risk customers is performed at least once a year. In addition, updating the customer information can be executed out when the customer performs significant actions (for example, resuming use of the bank's services, opening a new account), as well as revealing changes in the customer's management bodies, composition of its owners, etc.

Chapter 6. ANALYSIS OF TRANSACTIONS AND MONITORING CUSTOMERS' PERFORMANCE

57. The main stages in the monitoring of customers' performance are the following:

identification of transactions and activities of customers that require further study;

analysis of reports on such transactions by a responsible bank employee; making appropriate decisions on further study of customers' performance in reliance upon the results of the analysis.

58. Herein, particular attention is paid to the following parameters:

account user;

volume and number of transactions passing through the account; sources of funds;

the form in which funds have been deposited or withdrawn (cash, checks, etc.);

identity of the person making a transaction;

place of funds' direction;

transaction purpose certificate

customer relations with the bank employees;

other necessary information regarding the activities of the customer.

59. In case, that any facts are detected that, in the opinion of the bank's responsible officer, contribute to money laundering or he has suspicions about the legality of the transaction, the responsible officer makes appropriate notes and notifies the bank's management.

Chapter 7. ASSESSING THE RISK LEVEL

60. In order to determine, assess and reduce the risk level, the bank must undertake measures to study, analyze, identify, assess, monitor, manage, formalize and reduce the risk level.

In its performance the bank is obliged to systematically, at least once a year, make research, analysis and identification of possible risks of money laundering, terrorism financing and financing the proliferation of mass destruction weapons, confirming the research results by documents.

The bank must determine the general level of risk, required level of its reduction and implement an appropriate program of measures depending on the types and level of risks.

The measures applied should enable the decision to be made on the implementation of expanded or simplified measures to control the identified risks and efficient distribution of resources.

The risk level is identified and assessed by the assigned employees of the department for the

branches, based on information submitted by the customer taking into account the types of activities and transactions performed by the customer, the criteria established by the Internal Rules, the results of the customer due diligence, risk factors (by types and activities of customers, banking facilities and services , supply channels, geographical regions and others), including based on the study and analysis of the information provided by the customer.

The procedure for the implementation of measures to study, analyze, identify, assess, monitor, manage, document and reduce the risk level is established by internal rules.

61. With the aim of reducing the risks associated with the involvement of the bank, as well as the participation of its employees in illegal activities, including money laundering and terrorism financing or financing of the proliferation of mass destruction weapons, the bank determines the criteria used to assess the risk.

62. In reliance upon the information received in the process of the customer due diligence, taking into account the types of activities and transactions of the customer, the bank assesses and assigns an appropriate (high or low) risk level for the customer of making transactions with the aim of money laundering, or terrorism financing or financing proliferation of mass destruction weapons.

63. By identifying and assessing risks, the bank determines and uses the criteria, taking into account that the basic areas of assessment are the following:

customer base;

products and services offered by the bank;

geographic regions of the bank performance.

64. In order to reduce risks, the bank undertakes the following measures:

customer due diligence;

collection of additional information about customers;

analysis of transactions and monitoring of customer activities.

65. When a customer or a transaction made by a customer is included in the high-risk category, the bank must constantly monitor the transactions made by that customer.

66. As the nature of the transactions made by the customer changes, the bank, if necessary, should review the level of risk of working with it. The bank should pay a particular attention to all complicated, unusually major transactions, as well as to all extraordinary transaction schemes that do not have an explicit economic or visible legitimate purpose.

The results of the risk assessment should be submitted to the Central Bank of the Republic of Uzbekistan.

Chapter 8. SENDING MESSAGES TO THE DULY AUTHORIZED PUBLIC BODY (DAPB)

67. Upon admitting a customer's transactions as suspicious, the bank's responsible officer decides on the bank's further actions regarding the customer, including:

on submitting messages about a suspicious transaction to the DAPB: on the notification of the relevant managers of the bank (branch) and subdivisions directly working with customers, on admitting the transaction as suspicious;

on obtaining additional information about the customer;

on reviewing the risk level of working with a customer;

on the necessity for particular attention to transactions with the customer.

68. A responsible employee of the bank has the right to make proposals to the management of the bank (branch) on the termination of contractual relations with the customer in compliance with the law and the agreement concluded therewith.

69. A message about a suspicious transaction is forwarded by the bank to the DAPB not later than one business day following the day of detection, in compliance with the procedure determined by the national legislation.

70. A message to the DAPB is forwarded exclusively by the head office of the bank.

Chapter 9. STORAGE OF INFORMATION AND REPORTING ON CONTROL OUTCOMES

71. The bank must store:

information and documents containing the data related to the customer;

information about transactions, including information on which a message was forwarded to the DAPB;

reports of the responsible employee;

information on the employees' training.

72. With the aim of restricting access to documents (correspondence with the Central Bank and the DAPB, including paper and electronic copies of messages sent to the DAPB; paper and electronic customer profiles; journals, etc.) used in the activities of the department (responsible officer), such documents and their inventory should be stored directly by the internal control department (responsible officer) in specially equipped rooms or in a fireproof and sealed safe within the periods established by law, but not less than five years after the termination of business relations with the customers.

73. Hard copies of documents must be archived based on software, recorded on electronic media and stored by the director of the department, together with the list in a fireproof and sealed safe.

After the expiration of the storage period, the documents are handed over to the bank's archive according to the established procedure.

74. With the aim of assessing the risks associated with money laundering and terrorism financing or financing the proliferation of mass destruction weapons, a responsible officer submits a report to the chairman of the Executive Board on a quarterly basis on the outcomes of the implementation of the internal control rules to counter money laundering and terrorism financing or financing the proliferation of mass destruction weapons.

Chapter 10. PROCEDURE FOR TRAINING THE BANK'S EMPLOYEES ON THE ISSUES OF COUNTERING MONEY LAUNDERING AND TERRORISM FINANCING

75. The bank arranges training for employees on the issues of countering money laundering and terrorism financing or financing the proliferation of mass destruction weapons in the following areas on the basis of a plan for the training program implementation at "Kapitalbank" JSCB approved by the Executive Board of the bank:

a) familiarization of the bank employees with the statutory and other acts in the area of countering money laundering and terrorism financing;

b) familiarization of the bank employees with the rules of internal control in order to counter money laundering and terrorism financing approved by the Council of the bank;

c) training and rendering advisory services to the bank employees on the implementation of the legislation of the Republic of Uzbekistan in the area field of countering money laundering and terrorism financing.

76. Training programs are based on the fact that the basic condition for the bank to successfully implement activities to counter money laundering and terrorism financing is direct participation of each employee in this process within his competence.

77. The aim of training bank employees is to acquire the knowledge they need to comply with the requirements of the legislation of the Republic of Uzbekistan in the area of countering money laundering and terrorism financing, as well as those required for their implementation of the statutory acts of the Republic of Uzbekistan and the Central Bank in the area of countering money laundering and terrorism financing or financing of the proliferation of mass destruction weapons of and relevant internal documents of the bank.

78. The implementation of the Procedure is executed in part by adopting in the bank of the Technical Study Plan for each half-year. The plan contains a list of topics for technical studies, the dates and names of the officials responsible for the training. The plan is approved by the chairman of the Executive Board of the bank not later than January 15 and July 15 of the current year. If necessary, during the year, the Plan may be amended and supplemented by the chairman of the Executive Board.

79. Bank employees participate in the training program with the account of their functions.

Employees, engaged in attracting and servicing the customers, making calculations, are trained taking into account their functional responsibilities. Training programs include an explanation of the need to apply customer due diligence procedures, obtain additional information about the customer and monitor his activities.

80. Training of employees in countering money laundering and terrorism financing is also implemented when transferring to another job within the bank or when changing the functional duties of employees.

Chapter 11. ENSURING CONFIDENTIALITY

81. The Bank restricts access to the information related to countering money laundering and terrorism financing or financing the proliferation of mass destruction weapons, ensures its non-spreading and does not have the right to inform legal entities and individuals about submitting the messages about their transactions to the DAPB.

82. The bank shall ensure non-disclosure (or use for personal purposes or in favor of third parties) by its employees of the information acquired in the process of fulfilling their internal control functions.

83. The transfer of the information, including from the questionnaire, which constitutes the customer's identification data, to third parties is made in compliance with the applicable law.

84. This Policy shall enter into force upon its approval by the Council of "Kapitalbank" JSCB.

Introduced:		
Director of the Internal Control department	*signature*	Khasanov K.A.
Agreed:		
Chairman of the Executive Board	*signature*	Kim O.R.
Deputy Chairman of the Executive Board	*signature*	Rakhmatov B.S.
Deputy Chairman of the Executive Board	*signature*	Tyan K.V.
Deputy Chairman of the Executive Board	*signature*	Glushchenko A.P.
Deputy Chairman of the Executive Board	*signature*	Gimadiev S.A.
Chief accountant	*signature*	Allayorova D.N.
Director of Risk Management department	*signature*	Kan T.V.
Director of Legal service department	*signature*	Pachurin V.V.
Acting director of Internal audit department	*signature*	Yuldashev J.S.

Перевод выполнен переводчиком **Усмановым Маратом Ринатовичем.**
Владелец паспорта серии АА № 3139692, выданного 14.10.2013 г. УВД Чиланзарского района, города Ташкента. Переводчик не несет ответственности за содержание прилагаемого оригинала документа.
Об ответственности за ложный перевод предупрежден.

Translated by translator **Usmanov Marat Rinatovich.**
Holder of passport AA No. 3139692, issued on 14.10.2013, Chilanzar District Department of Internal Affairs of Tashkent.
The translator is not liable for the content of the attached original document.
The translator has been warned on liability for a false translation.

На основании статьи 67 Закона Республики Узбекистан «О нотариате», нотариус, свидетельствуя подлинность подписи, не удостоверяет факты, изложенные в документе, а лишь подтверждает, что подпись сделана определенным лицом.

Республика Узбекистан.
Город Ташкент.
«28» Января две тысячи двадцатого года.

Я, **ЭРГАШЕВ ВАЛИШЕР АЛИШЕРОВИЧ,** нотариус государственной нотариальной конторы № 1 Чиланзарского района, города Ташкента, свидетельствую подлинность подписи известного мне переводчика УСМАНОВА МАРАТА РИНАТОВИЧА. Личность подписавшего документ установлена, дееспособность проверена, т.е. при личном общении с ним, его дееспособность сомнений не вызвала.

Зарегистрировано в электронном реестре за № 202000108000835

Взыскано государственной пошлины 44 600с. 00 т.

НОТАРИУС ЭРГАШЕВ В.А.

Гербовая печать:
Министерство Юстиции Республики Узбекистан
Управление юстиции города Ташкента
Государственная нотариальная контора № 1
Чиланзарского района
НОТАРИУС
В.А. ЭРГАШЕВ

On the basis of Article 67 of the "Law of Notary Public", the Notary attesting the genuineness of signature, does not certify the facts recited in the document, but only confirms that the signature is made by certain person.

Republic of Uzbekistan. Tashkent City

«28» of January of two thousand and twentieth year.

I, **ERGASHEV VALISHER ALISHEROVICH**, Notary of State Notary's Office No. 1 of Chilanzar District, Tashkent City, hereby certify the authenticity of signature made by known to me translator USMANOV MARAT RINATOVICH. The Personality of signed person is established.

Registered in the Register under No. № 202000108000835
Paid State Duty 44 600s. 00 т

NOTARY (signed) ERGASHEV V.A.

Official Emblem seal of Notary