INTERNAL REGULATIONS FOR COMBATING MONEY LAUNDERING, AND FINANCING OF TERRORISM OR FINANCING OF PROLIFERATION OF WEAPONS OF MASS DESTRUCTION AT «ASIA ALLIANCE BANK»JSCB

Tashkent -2023

INDEX

I. GENERAL

1. These Regulations are developed in accordance with the laws of the Republic of Uzbekistan "Concerning Banks and Banking Activities" dated August 30, 2003, "Concerning Banking Secrecy", "Concerning Anti-Money Laundering and financing of terrorism"; "Regulations on the procedure for submitting information related to Anti-Money Laundering and financing of terrorism" (Annex No. 1 to No. 402 Resolution of the Cabinet of Ministers of the Republic of Uzbekistan dated June 29, 2021), Internal Regulations concerning Anti-Money Laundering and financing of terrorism in commercial banks" (hereinafter referred to as Internal Regulations), registered on May 23, 2017 with the Ministry of Justice under No. 2886, "Regulations on Digital Identification of Customers", registered on September 30, 2021 with the Ministry of Justice under No. 3322 , "Regulations on the procedure for suspending operations, freezing funds or other property, providing access to frozen property and resuming operations of persons included in the list of persons participating or suspected of participating in terrorist activities or proliferation of weapons of mass destruction", registered on October 19, 2021 with the Ministry of Justice under No. 3327.

   These Regulations define the procedure for organizing and implementing internal control in order to counteract Money Laundering and financing of terrorism at "ASIA ALLIANCE BANK" JSCB (hereinafter referred to as the Bank), as well as the procedure for suspending operations, freezing funds or other property, providing access to frozen property and resumption of operations of persons included in the list of persons involved or suspected of participating in terrorist activities or proliferation of weapons of mass destruction.

2. The following basic concepts shall be used in these Regulations:

   Internal control means activities of a commercial bank for customers due diligence, managing the risks of money laundering, financing terrorism and financing proliferation of weapons of mass destruction, identifying dubious and suspicious transactions, as well as transactions involving persons participating or suspected of participating in terrorist activities or proliferation of weapons of mass destruction;

   Internal control system is a set of actions of the Internal Control Service and other divisions of a commercial bank aimed at achieving the goals and fulfilling the tasks defined by these Regulations and internal documents;

   Internal Control Service is a special subdivision of a commercial bank responsible for the implementation of internal control;

   Employees of the Internal Control Service are employees of the Internal Control Service of the Head Office of a commercial bank, a responsible officer or head and employees of the Internal Control Service of a branch of a commercial bank responsible for internal control;

   Manager of the Internal Control Service means Head of the Internal Control Department directly supervising implementation of the activities of the internal control system in the bank based on the internal control Regulations, being the Head of employees of the Internal Control Service;

   Designated Authority means the Department for organized crime, economic crime and corruption at the General Prosecutor's Office of the Republic of Uzbekistan (hereinafter - the Department);

   Customer is an individual or legal entity that has applied to a commercial bank with a request (application, petition) to carry out a transaction with funds or other property (hereinafter referred to as transactions);

   Beneficial owner is a person who ultimately owns the property rights or effectively controls the customer, and for whose benefit the transaction with funds or other property is performed;

   Dubious transaction means transaction in respect of which a commercial bank, in the process of exercising internal control, had doubts about its implementation in order to legalize proceeds from crime, financing terrorism and (or) financing proliferation of weapons

of mass destruction, before making a decision on inclusion (non-inclusion) it to the category of suspicious transactions;

Suspicious transaction is a transaction that is in the process of being prepared, committed or has already been committed, in respect of which a commercial bank, in the process of exercising internal control, has a suspicion that it is being carried out in order to legalize proceeds from crime, financing terrorism and (or) financing proliferation of weapons mass destruction;

One-time transaction means transactions carried out by customers on a one-time basis without opening a bank account, not repeated for at least one month;

Customer Due Diligence means verifying the identity and authority of the customer and those on whose behalf the customer is acting, identifying the beneficial owner of the customer, and conducting ongoing reviews of the customer's business relationships and transactions to verify that they are consistent with the details of the customer and its activities;

Customer identification means determination by a commercial bank of data about customers based on the documents provided by them, additionally confirmed information available in open sources and databases in order to carry out customer due diligence;

Identification of the customer's beneficial owner means determination by the commercial bank of a legal entity of the owner, including the person controlling the customer by studying the structure of ownership and management based on the constituent documents determined by law (Articles of Association and (or) Memorandum of Association, Regulations);

States not participating in international cooperation in the field of anti-money laundering and financing of terrorism means states and territories identified in the official statements of the Financial Action Task Force on Money Laundering, which pose a threat to the international financial system and whose system for anti-money laundering and financing of terrorism has strategic shortcomings;

Offshore zone are states and territories that provide a preferential tax regime and (or) do not provide for the disclosure and presentation of information when conducting financial transactions;

Risk is the risk of customers making transactions for the purpose of money laundering, financing terrorism or financing the proliferation of weapons of mass destruction;

Remote services are banking services provided for conducting transactions using programs that make it possible to carry out transactions without the customer appearing at the Bank.

Public officials are persons appointed or elected permanently, temporarily or by special authority, performing organizational and administrative functions and authorized to perform legally significant actions in a legislative, executive, administrative or judicial body, including military structures of a foreign state or in an international organization, as well as high-ranking heads of enterprises of foreign states, well-known politicians and well-known members of political parties of foreign states (including former ones);

Freezing of funds or other property means a ban on the transfer, conversion, disposal or movement of funds or other property;

Suspension of the operation means suspension of execution of the customer's instructions for transfer, conversion, transfer of funds or other property into possession and use of other persons, as well as performance of other legally significant actions;

Person involved or suspected of participating in terrorist activities means a natural or legal person who participates or is suspected of participating in terrorist activities, directly or indirectly owns or controls an organization that carries out or is suspected of carrying out terrorist activities, as well as a legal entity that is located owned or controlled by a natural person or organization carrying out or suspected of carrying out terrorist activities;

A person participating or suspected of participating in the proliferation of weapons of mass destruction is an individual or legal entity, determined by Resolutions of the UN Security Council and international legal documents recognized by the Republic of Uzbekistan, aimed at preventing proliferation of weapons of mass destruction;

List means a list of persons participating or suspected of participating in terrorist activities or proliferation of weapons of mass destruction, generated by the Department based on the information provided by state bodies engaged in the fight against terrorism, proliferation of weapons of mass destruction, and other competent authorities of the Republic of Uzbekistan, as well as information, received through official channels from the competent authorities of foreign states and international organizations.

Third party means organizations registered in the Republic of Uzbekistan and carrying out transactions with funds or other property specified in Article 12 of the Law of the Republic of Uzbekistan "Concerning anti money laundering, financing of terrorism and financing of proliferation of weapons of mass destruction";

Foreign structure without establishing a legal entity is an organizational structure established in accordance with the legislation of a foreign state without establishing a legal entity and having the right to carry out activities aimed at generating income (profit) in the interests of its participants (shareholders, trustees or other persons) or other beneficiaries (funds, partnerships, communities, trusts, other forms of collective investment and (or) trust management).

Payment agent is a legal entity that is not a bank entered into an agency agreement with a bank or a payment organization for the provision of payment services;

Payment subagent is a legal entity that is not a bank, or an individual entrepreneur who has entered into a sub-agency agreement with a payment agent for the provision of payment services;

Digital identification means the process of checking and verifying identity of the customer using information systems in accordance with the requirements established by the Regulation "Concerning Customers Digital Identification";

Digital authentication means the process of checking and verifying identity of the customer by automated (without human factor) comparison of photos or videos taken in real time from a previously identified customer with the original identification data;

Contact Center (hereinafter referred to as the Center) is a division of the Bank or a service that receives and processes telephone calls, SMS and e-mail messages, as well as messages via chats and social networks or through other channels to inform about the products and services of the Bank, and other functions determined by the Bank for Customer service;

II. CUSTOMER DUE DILIGENCE

2.1. General Provisions for Customer Due Diligence

2.1.1. Customer due diligence is one of the measures aimed at anti money laundering and financing of terrorism. Customer due diligence shall be carried out in order to know at the proper level who and for what purpose carry out operations in the Bank.

2.1.2. The relevant divisions of the Bank shall independently take measures for customers due diligence in the following cases:

a) when establishing business and civil law relations, including:
- when a legal or natural person applies for opening a bank account (deposit);
- when an individual applies for a bankcard;
- when legal entities and (or) individuals apply for the purchase of securities issued by a commercial bank;
- when legal entities and (or) individuals own shares of a commercial bank, for an amount equal to or greater than one percent of its authorized capital;

- when an individual applies for a loan or a service for storing valuables in a bank deposit box;

b) when carrying out one-time transactions, including through the performance of one or more transactions related to each other, in the following cases:
   - receipt of foreign currency by customer from the bank cash desk in cash on bank cards issued by other banks, in an amount equal to or exceeding 100 times the size of the Reference Calculation Value;
   - purchases of foreign currency by individuals in an amount exceeding 100 US dollars in equivalent;
   - carrying out a transaction without opening or using a bank account for an amount equal to or greater than 500 times the Reference Calculation Value;
   - when making or receiving money transfers provided for in clause 2.6.8 of these Regulations;

c) if there are suspicions of money laundering and financing of terrorism, regardless of any exceptions established by these Regulations;

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

Payment agents and payment sub-agents may verify the identity and identification of customers in order to apply customer due diligence measures, subject to the requirements of the legislation on combating money laundering, financing of terrorism and the financing of proliferation of weapons of mass destruction, in cases where this is provided for by the agency and (or) sub-agency agreement.

2.1.3. Customer due diligence measures taken by the Bank's employees must include:

- verification of the customer's identity and identification;
- identification, verification of the identity and authority of a person acting on behalf of the customer, based on relevant documents;
- identification of the customer's beneficial owner;
- studying the purpose and nature of the business relationship or planned transactions;
- carrying out on an ongoing basis an examination of the business relationships and transactions carried out by the customer, in order to verify its compliance with information about such a customer and its activities, nature of the risk, including the source of funds, if required.

Banks are required to use risk management systems to determine whether a customer or beneficial owner is a public official and, together with the above measures on customer due diligence in relation to public officials acting as a customer or beneficial owner:

- take reasonable steps to verify information about the status of a public official and determine the source of funds or other property from transaction;
- establish (or continue for existing customers) business relations with a public official only with permission of the Chairman of the Management board of the bank or its authorized deputy;
- carry out continuous in-depth monitoring of business relations.

The Bank should apply the above measures also to family members of public officials or persons close to public officials.

The Bank shall immediately notify the Department of the planned transactions related to generation of sources or other property, and at the same time meeting the criteria specified in clause 3.1.2 of these Regulations, and shall conduct such transactions within no more than three business days after carrying out a full analysis in order to identify the level of risk of its interconnectedness.

2.1.4. In the event that legal entities and individual entrepreneurs, whose founders are residents of the Republic of Uzbekistan, apply for the remote opening of a bank account in the process of passing their state registration, the measures for customer due diligence provided for in paragraph two Clause 2.1.3 of these Regulations, can be carried out by the Public Service Centers (hereinafter referred to as the registering authority) and the

bank can trust the results of the measures taken. In doing so, the bank must ensure:

- in the possibility of immediately obtaining the necessary information on the measures of customer due diligence through the automated system of state registration and registration of business entities;
- in compliance with the requirements for conducting customer due diligence measures established in legislative acts by the registering authority.

In case of non-compliance with the requirements specified in paragraphs two and three of this clause, commercial banks shall independently carry out measures for customer due diligence.

When carrying out customer due diligence measures by the registering authority, the decision to enter into business relations with a customer shall be made by a commercial bank independently, based on risk. At the same time, the offer of the Bank Account Agreement must specify the possibility of carrying out measures for customer due diligence by commercial banks.

2.1.5. Commercial banks may trust the results of customer due diligence carried out by third parties in accordance with the due diligence measures specified in paragraphs two to four Clause 2.1.3 of these Regulations. In such cases, the ultimate responsibility for customer due diligence rests with the commercial bank. At the same time, commercial banks must make sure:

- in the possibility of immediately obtaining (by means of electronic systems) the necessary information for customer due diligence;
- to be able, upon request, to immediately obtain copies of identification data and other relevant customer due diligence documents;
- that third parties are guided by internal rules on combating money laundering, financing of terrorism and financing of the proliferation of weapons of mass destruction.

In the event of non-compliance with one of the requirements provided for in paragraphs two to four of this clause, commercial banks must independently take measures for customers due diligence.

Commercial banks shall decide to enter into a business relationship with a customer independently, based on risk, and entitled to take due diligence measures.

Commercial banks must stipulate the possibility of taking measures for customers due diligence in the contract and (or) in the offer agreement.

2.1.6. When a customer, or a transaction by a customer, is classified as high-risk, banks should apply the following enhanced due diligence measures to that customer:

- collection and recording of additional confirmed information about the customer, available in open sources and databases;
- obtaining from the customer information about the sources of funds or other property for the operations carried out by it;
- study of the planned operations purposes or carried out by such customer;
- conducting continuous monitoring of the ongoing operations of such customer.

If it is not possible to apply enhanced measures for customer due diligence, in particular, obtaining from the customer information about the sources of funds or other property on the operations carried out by it and (or) studying the purposes, planned or conducted operations by such customer the bank must send a message about this to the Department and refuse to enter into a business relationship with such a customer or conduct transactions of such a customer.

2.1.7. All documents that allow identifying the customer and other participants in the transaction must be available on the date of its submission.

2.1.8. If employees of the respective divisions of the Bank have suspicions about reliability of the information (documents) received from customers, it is necessary to take measures

to check (verify) this information (documents). In these cases, the Bank's divisions may apply to the relevant organizations to determine reliability (validity) of information (documents) about customers.

2.1.9. The Bank should apply due diligence measures to existing customers, taking into account the significance and risks, and at the appropriate time, conduct due diligence on existing relationships, taking into account when and in general such reviews are carried out or not carried out, as well as the sufficiency of the data obtained.

2.1.10. Re-identification of the customer and real owner of the customer should be carried out in case of doubts about the accuracy of information obtained as a result of the previous identification.

2.1.11. When identifying a customer and beneficial owner of a bank customer, including when it acts through its payment agents and (or) payment subagents, the Bank should verify the information received with the List, as well as with the list of states not participating in international cooperation in the field of combating money laundering, financing of terrorism and financing of the proliferation of weapons of mass destruction, generated and provided to commercial banks by the Department in accordance with the procedure established by law.

If, during identification of the customer and beneficial owner of the customer, persons included in the List are identified, the Bank should take the measures specified in clauses 6.1.1–6.1.4 of these Regulations.

2.1.12. The Automated Banking System (ABS) available in the Bank, when entering customer identification information into the ABS, should allow automatic verification with the List and other data in the ABS (UN, Office of Foreign Assets Control of the US Department of the Treasury (OFAC SDN List) etc.), as well as to identify and report them. If there is no possibility for automatic reconciliation, employees of the relevant department must check it themselves with the lists in the spreadsheet.

2.1.13. The Bank has the right to refuse the customer to carry out transactions in the following cases:

- absence at its location (postal address) of a management body of a legal entity or a person entitled to act on behalf of a legal entity without a power of attorney;
- provision of knowingly unreliable documents or failure to provide documents requested in accordance with the law;
- in other cases stipulated by the legislation.

2.1.14. The Bank is prohibited to:

- open accounts (deposits) for anonymous owners, that is, without providing by individuals or legal entities that open the account (deposit) the documents necessary for its identification;
- open accounts in clearly fictitious names that are not documented;
- open accounts without personal presence of the person opening the account or his authorized representative, except in cases where the bank is able to identify the customer based on the previously submitted documents that are valid and verified on the date of identification, as well as customer due diligence measures have been taken by the registration authority, or the bank, on the basis of biometric data, as well as the commercial bank, shall trust the results of customer due diligence carried out by a third party;
- establish and continue relations with non-resident banks that do not have a physical presence and permanent management bodies in the territories of the states in which they are registered;
- issue of securities and other financial instruments to bearer;
- provide services for receiving and sending funds in foreign currency, including through international money transfer systems, without identifying the customer;
- establish subsidiaries, branches or representative offices on the territory of states that do not participate in international cooperation in the field of combating money

laundering and financing of terrorism.

2.1.15. If it is not possible to carry out a customer due diligence, a commercial bank, including when it acts through its paying agents and (or) subagents, must inform the Department about this and refuse to enter into business relations with such a customer or conduct transactions of such a customer or terminate any business relationship with him.

2.1.16. Managers of the relevant departments are responsible for ensuring that customer due diligence and completion of electronic questionnaires are carried out in a timely and correct manner.

Branch managers are responsible for overseeing customer due diligence and completing its electronic forms.

2.2. Identification of Individuals

2.2.1. Identification of a customer - an individual corresponding to the Bank's divisions shall be carried out based on an identity document (passport or a substitute document) or biometric data. In this case, the bank, when identifying a customer - individual:

- based on an identity document (passport or a document replacing it), must check the original of such a document;
- based on biometric data, must verify such data with the information system of the Ministry of Internal Affairs of the Republic of Uzbekistan.

Information received as a result of identification of an individual - customer, shall be entered into an electronic questionnaire on the day of the operation.

2.2.2. Identification of a customer - individual in the Bank shall be carried out based on the information provided for in Annex No. 1 to these Regulations, as well as documents that are the basis for transactions and other transactions, and other necessary information.

2.2.3. When a customer - individual applies to the Bank to open a savings account, a responsible officer of the Retail Services Department, when applying for a bank plastic card or performing operations through the terminal located in the Bank (cash withdrawal, payment for goods and services) using a plastic card, with the exception of utility bills, communication services, payments to the budget, extra-budgetary funds and other obligatory payments - the responsible officer of the Retail Services Department, when applying for a loan - a responsible officer of the Credit Operations Department, when applying for one-time transactions conducted through the Bank's cash desk, if the implementation of this one-time operation requires customer identification based on these Regulations, a responsible employee of the Cash Operations Department, who is entrusted with the corresponding function, shall identify the customer.

Manager of the Cash Operations Department shall be responsible for ensuring identification of the customer for a one-time transaction carried out by it through the Bank's cash desk, and filling out its electronic questionnaire.

2.2.4. When a customer - individual applies with an application at the banking services center to open a savings account, when applying for a bank plastic card or performing operations through the terminal located in the Bank (cash withdrawal, payment for goods and services) using a plastic card, except for payment utilities, communication services, payments to the budget, extra-budgetary funds and other obligatory payments, a responsible employee of the banking service center shall identify the customer.

2.2.5. When a customer applies to the Bank to perform a one-time operation, if the implementation of this one-time operation requires customer identification based on these Regulations, a responsible officer shall, in order to identify the customer, after reviewing the original document confirming his identity, check the availability of the customer’s electronic questionnaire in the ABS. In the absence of an electronic customer profile, a responsible officer shall take a copy of the document confirming his identity and, based on the identification information received, form an electronic customer profile, specifying the date and type of operation.

Moreover, if there is an electronic customer profile, a responsible officer shall check

compliance of the information in the document confirming his identity with the information in the electronic questionnaire. With a complete match of the information, it is not required to obtain a copy of the document confirming the customer's identity. And, if the information does not match for some reason (the document has been updated, the address has been changed, etc.), a responsible officer shall take a copy of the identity document and make appropriate changes to the customer's electronic questionnaire.

2.2.6. The information obtained as a result of customers due diligence who have performed one-time transactions shall be updated when performing subsequent transactions that require acceptance of customer due diligence.

2.3. Identification of individual entrepreneurs, as well as legal entities and their real owners

2.3.1. Identification of an individual entrepreneur, a legal entity and its real customer in the Bank shall be carried out based on the information provided for in Annex No. 2 to these Regulations, as well as documents that are the basis for transactions and other transactions, and other necessary information.

2.3.2. When performing customer due diligence measures in relation to customers - legal entities and individual entrepreneurs, the Corporate Services Department for Legal Entities must obtain from them the relevant documents on state registration, information about managers, as well as information specified in the constituent documents.

Obtaining the specified information shall be carried out through an automated system of state registration and registration of business entities or directly from the customer in the event that when it is impossible to obtain information from this system.

As part of the due diligence process for legal entities, the Corporate Services Department for legal entities shall take reasonable and accessible steps to identify an individual who is a beneficial owner of the customer and who ultimately owns or controls the customer, including by examining:

- ownership and control structure of the customer, and founders (shareholders, participants) of the customer.
- ownership and management structures of the customer;
- founders of the customer (shareholders/participants owning at least ten percent of the shares/stakes of the company);
- personal data of an individual (persons) who ultimately owns a share (at least ten percent) of a legal entity (if any);
- if doubts arise as a result of the measures taken as to whether the person (persons) holding the controlling interest is the beneficial owner or in the absence of persons exercising control over the ownership of the shares, the personal data of the natural person (persons) exercising control over the legal entity through other methods (if any).

If it is not possible to identify the beneficial owner by the appropriate measures taken by commercial banks, the bank must identify the person holding a high management position and take reasonable steps to verify his identity.

2.3.3. If a customer or the beneficial owner of the customer is a legal entity that is subject to the requirements of regulatory legal acts on the disclosure of information on the structure of ownership, then identification and confirmation of the identity of the founders (shareholders owning at least ten percent of the company shares, participants) of such a legal entity is not required.

2.3.4. For foreign structures without establishing a legal entity, the requirements established by these Regulations for legal entities shall be applied.

2.3.5. In order to study the customer - legal entity more carefully, special attention should be paid to:

- composition of founders (shareholders, participants) of the customer, definition of persons holding shares of more than 10 percent of the authorized capital (fund) of the

customer;

- structure of the customer's management bodies and their powers;
- size of the customer’s registered authorized capital (fund).

2.3.6. When a customer - legal entity or an individual entrepreneur applies to the Bank for a loan, a responsible officer of the Credit Operations Department must carry out its due verification and verify identification information with the data in the questionnaire. If the data in the customer's electronic questionnaire differs from the information provided by the customer, a responsible officer of the Credit Operations Department shall inform the Manager of the Customer Service Department and an employee of the Internal Control Service about this.

2.3.7. Customer due diligence information must be updated at least once a year in cases where the Bank assesses the risk of the customer's money laundering, terrorist financing and financing of proliferation of weapons of mass destruction as high, otherwise not less than once every two years and if there are changes in the customer's information.

In order to update the customer’s identification information available in the Bank, Manager of the Corporate Services Department for Legal Entities shall, by the end of the month, draw up a list of customers who have been assigned a high risk level from the date of the last identification for one year and two years for other customers and distribute them to responsible employees.

Responsible employees within one month shall take measures to study and update the real identification information of the customers specified in this list.

2.3.8. When making changes to the existing customer identification information, a relevant employee of the Corporate Services Department for Legal Entities must make the appropriate changes to the customer's questionnaire and inform an employee of the Internal Control Service about this.

2.3.9. Manager of the Corporate Services Department for Legal Entities shall be responsible for the timely and correct performance of duties for customer due diligence of legal entities and individual entrepreneurs and filling out their electronic questionnaires.

2.4. Carrying out in-depth monitoring for establishment of business relations with public officials and their close relatives, as well as their transactions

2.4.1. In addition to applying the above customer due diligence measures, in relation to public officials acting as a customer or beneficial owner of a customer, Bank employees must:

- take reasonable measures to verify information about the status of a public official and determine the source of funds or other property for the operation;
- establish (or continue for existing customers) business relations with a public official only with permission of the Chairman of the Management board of the bank or his authorized deputy;
- carry out continuous in-depth monitoring of business relations.

2.4.2. In the course of customer due diligence, the account manager must take reasonable and accessible steps to verify that the customer and persons acting on behalf of the customer, the customer's beneficial owner, are public officials. At the same time, verification of the customer and persons acting on behalf of the customer, as well as beneficial owner of the customer for belonging to public officials shall be carried out before establishing a business relationship with the customer, based on the information obtained during identification.

To do this, a responsible officer, if the customer and persons acting as a customer, beneficial owner of the customer are not citizens of the Republic of Uzbekistan, or are legal entities registered in other states, should pay attention to their name, obtain additional confirmed information from open sources and databases data, if necessary, contact an employee of the Internal Control Service of the branch for additional information.

If it is established that the customer and persons acting as a customer, beneficial owner of the customer are public officials, a responsible officer of the relevant department,

before establishing a relationship with the customer and or carrying out its transactions, must immediately inform the Branch Manager and an employee of the Branch Internal Control Service about such customer in writing. In turn, the Branch Manager must inform the Chairman of the Management Board or his authorized deputy about the public official in writing, and ask for appropriate instructions on entering into relations with him.

2.4.3. An employee of the Branch Internal Control Service, after receiving a message from a responsible employee about identification of a public official, must inform the Manager of the Internal Control Service about this. The Internal Control Service, after receiving a notification that the customer and persons acting as a customer, beneficial owner of the customer are public officials, must take the following measures:

- to the extent possible, identify in detail identity of the customer and beneficial owner of the customer, as well as obtain additional information about the customer from public databases or through basic programs of special persons;
- take measures to identify the source of the customer's funds or his financial position, including through obtaining information from the customer;
- assign a high level of risk to the customer;
- assess the risk of establishing a relationship with a customer and carrying out its operations;
- report the identified public official to the Chairman of the Management board or his authorized deputy;
- consider reporting to the Department on the operation of a public official;
- strengthen monitoring of customer transactions.

2.4.4. Chairman of the Management board or his authorized deputy, no later than the day the notification is received, must give an appropriate instruction on establishing or not establishing relations with a public official.

A corresponding instruction shall be immediately communicated in the prescribed manner to the Branch Manager and responsible employees. If the instruction states the need to establish relations with the customer, the Branch Manager and responsible employees shall establish relations with the customer. Enhanced customer due diligence measures shall be applied for public officials.

2.4.5. Employees of the Branch Internal Control Service as an additional measure to identify public officials, if the customer and persons acting as a customer, beneficial owner of the customer are not citizens of the Republic of Uzbekistan, or are legal entities registered in other states, should pay attention to their name, obtain additional confirmed information about the customer from open sources and databases, as well as control the implementation of the identification of public officials by responsible employees in the prescribed manner.

2.5. Due Diligence of Non-Resident Banks when Establishing and Implementing Correspondent Relations

2.5.1. When establishing and implementing correspondent relations with a non-resident bank, the identification of a non-resident bank shall be carried out by the Foreign Economic Affairs Department.

2.5.2. When identifying, the Foreign Economic Affairs Department must:

- ensure that a bank acting as a transit financial institution, in cases where technical limitations prevent the required originator and beneficiary information associated with an international wire transfer from being retained, associated with an international wire transfer, should keep records of all information received from the originating financial institution or another transit financial institution, for at least five years.
- collect information about a non-resident bank in order to get a complete picture of the nature of its business activities;
- determine, on the basis of open information, the reputation and quality of supervision, including whether this bank has been investigated for violations related to money laundering, financing of terrorism and financing of the proliferation of weapons of

mass destruction, or whether measures have been taken against it by regulating bodies;

- assess the measures taken by a non-resident bank to combat money laundering, financing of terrorism and financing of the proliferation of weapons of mass destruction;
- in relation to "transit accounts" - receive appropriate confirmation that the respondent bank has fulfilled the obligation to conduct due diligence in relation to its customers who have direct access to the accounts of the correspondent bank, as well as the possibility of providing, at the request of the correspondent bank, the necessary data about the customer received as a result of identification;

The decision to establish correspondent relations with a non-resident bank shall be made by the Management Board of the Bank.

2.5.3. A Foreign Economic Affairs Department must send to the non-resident bank with which correspondent relations are established requests for the possibility of providing the necessary information regarding necessary identification for the implementation of activities to combat money laundering and financing of terrorism, and take the necessary measures to obtain confirmation.

2.5.4. A Foreign Economic Affairs Department must send to a foreign bank with which correspondent relations are established a questionnaire in the form specified in Annex No. 4 to these Regulations, if it is registered in the territory of the CIS states, and in the form specified in Annex No. 5 to these Regulations, if it is registered in territories of other states, and take the necessary measures for its return with confirmation.

The Foreign Economic Affairs Department shall provide the Internal Control Service with a color scanned copy of the confirmation and questionnaire received from a foreign non-resident bank.

2.5.5. The bank shall ensure that non-resident banks with which it establishes correspondent relationships apply international due diligence standards and apply appropriate due diligence procedures to transactions.

2.5.6. The decision to establish correspondent relations with a non-resident bank shall be made by the Management Board of the Bank.

2.5.7. The relevant divisions of the Bank, when establishing relationships with other banks for making transit transfers, must keep all information about electronic payments.

2.5.8. Ensuring a clear and complete distribution of responsibilities between correspondents of the Foreign Economic Affairs Department.

2.5.9. The Foreign Economic Affairs Department must take measures to reflect the relevant clauses in the agreements entered into with correspondent banks with non-residents in order to be able to obtain additional information about the senders of funds within three working days.

If this is not possible, the Bank should consider terminating the agreement with such non-resident correspondent banks.

2.5.10. When continuing correspondent relations with non-resident banks located on the territory of states that do not participate in international cooperation in the field of combating money laundering and financing of terrorism, or by its subsidiaries, branches and representative offices, the relevant divisions of the Bank, as well as the Internal Control Service should pay special attention to all transactions carried out with them.

The Bank shall:

- take measures aimed at preventing the establishment of relations with non-resident banks in respect of which there is information that their accounts are used by banks that do not have permanent management bodies in the territories of the states in which they are registered;
- when making international settlements, exchange payment details and other information related to the implementation of the above settlements with correspondent

banks;

- pay special attention and conduct a thorough 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, location (postal address) and account number of the sender) is not provided or is not provided in full.
- strengthen control over the activities of their foreign subsidiaries, branches and representative offices located in states that do not participate in international cooperation in the field of combating money laundering and financing of terrorism;
- require its foreign subsidiaries, branches and representative offices to inform the Head Office if it is impossible to apply appropriate measures to combat money laundering, financing of terrorism and financing of the proliferation of weapons of mass destruction due to the existing prohibition by acts of the legislation of the country, where it has subsidiaries, branches and representative offices. In turn, the Bank shall notify the Central Bank and the Department of this and take appropriate additional measures to manage the risks associated with money laundering, financing of terrorism and (or) financing of the proliferation of weapons of mass destruction.

2.5.11. If there is information about cases of violation by a non-resident bank of the requirements of international standards for combating money laundering and financing of terrorism, the Management Board of the Bank should consider responding appropriately, up to and including termination of cooperation with this correspondent.

2.5.12. These Regulations are binding on the payment agents of the Bank and its payment subagents, as well as all subdivisions and subsidiaries of the Bank's branches and representative offices abroad.

2.5.13. When executing an agency agreement with a paying agent, the Deposit and Transaction Operations Department of the Bank shall be responsible for including the requirement to comply with these Regulations in the agency agreement, as well as for controlling the inclusion of this requirement in sub-agency agreements executed between the paying agent and the paying subagent. The Deposit and Transaction Operations Department shall control delivery of a copy of these Regulations in paper or electronic form to the payment agent of the Bank.

2.6. Due diligence of companies providing international money transfer services through international money transfer systems and international plastic card systems, when establishing and implementing relations with them

2.6.1. Deposit and Transaction Operations Department and Card Business Department shall carry out identification of companies providing services in the system of international money transfers (hereinafter referred to as international money transfer systems), and companies providing services in the system of payments through international plastic cards (hereinafter referred to as international systems of plastic cards), when establishing relations with them.

2.6.2. The Deposit and Transaction Operations Department must, in addition to identification:

- collect information about a partner in international money transfers and international plastic cards in order to get a complete picture of the nature of its business activities;
- determine, on the basis of open information, reputation, including whether this organization has been investigated for violations related to money laundering and financing of terrorism;
- save all information about the electronic transfer.

2.6.3. The decision to establish relations with international money transfer systems and international plastic card systems shall be taken by the Management Board of the Bank.

2.6.4. The Deposit and Transaction Operations Department shall take the necessary measures to the systems of international money transfers and systems of international plastic cards when establishing relations, followed by sending at least once every two years a questionnaire in the form specified in Annex No. 4 to these Regulations, if it is registered in the territory of CIS and questionnaires in the form specified in Annex No. 5 to these

Regulations, if it is registered on the territory of other states, with its completion and confirmation.

2.6.5. The Deposit and Transaction Operations Department and Card Business Department shall provide the Internal Control Service with a color scanned copy of the questionnaire received from the international money transfer system and international plastic card system. The Internal Control Service may also request other information on the study of this system.

2.6.6. When carrying out money transfer transactions, as well as transactions through international money transfer systems, the Deposit and Transaction Operations Department must keep records of the divisions (branches, divisions, etc.) of the Bank providing such services and employees of these divisions.

2.6.7. The Deposit and Transaction Operations Department, together with divisions providing services for the implementation of international money transfers, should:

- ensure that money transfers are accompanied by accurate information about the customer-sender (name of the sender; series and number of the document (passport or equivalent document) proving identity - for individuals; account number, if the customer's account or a unique transaction code is used during the operation; sender's address or state identification number or customer's identification number or, for individuals, date and place of birth), and about the recipient (name of the recipient; account number, if the customer's account or unique transaction number is used during transaction);
- require non-resident banks and international money transfer systems to provide minimum information (name of the sender); account number, if the customer's account or a unique transaction number is used in the course of transaction) about the sender of funds, the amount of which does not reach 50 times the Reference Calculation Value;
- require non-resident banks and international money transfer systems to provide minimum information (name of the sender; series and number of the identity document (passport or equivalent document) - for individuals; sender's address or state identification number or identification number of the sender or for individuals date and place of birth; sender's account number, if the customer's account or a unique transaction number is used during transaction) about sender of funds, which amount is equal to or exceeds 50 times the Reference Calculation Value;
- take reasonable and accessible measures to identify international money transfers that do not have the required information about the recipient and (or) sender.

Electronic money transfers that do not contain the required information about the recipient or sender shall be refused by the responsible officer. In the event that additional information about the recipient and sender is obtained through customer or international money transfer systems, such money transfers should be carried out by responsible employees. The responsible person must notify employees of the Internal Control Service of such transfers. An employee of the Internal Control Service shall be required to review the level of risk for the transaction or customer and report this to the Department.

It is prohibited to provide money transfer services, including through international money transfer systems, if the money transfer does not meet the requirements established by this paragraph.

2.6.8. Data on outgoing domestic electronic money transfers, the amount of which is equal to or exceeds 36 times the Reference Calculation Value, must include information about the sender obtained during the customer identification and information about the recipient, in accordance with clause 2.6.7, unless complete information about the sender can be obtained using other sources. In such cases, the Deposit and Transactions Department shall include personal identification number of the individual, as well as the account number or unique transaction code (identifier), provided that this account number or identifier allows the transaction to be traced back to the sender or recipient.

The Deposit and Transaction Operations Department must ensure that internal electronic money transfers, which amount does not reach 36 times the Reference Calculation Value, are accompanied by information about the sender (name of the sender; sender's account number, when such an account or a unique transaction code is used in transaction) and about beneficiary (name of the beneficiary; beneficiary's account number, when such an account or a unique transaction code is used in transaction).

2.6.9. Information on domestic wire transfers must include information about the sender, as in the case of international money transfers.

The Deposit and Transaction Operations Department must take measures to reflect relevant clauses in agreements executed with international money transfer systems in order to be able to obtain additional information about the sender of funds within three working days.

If this is not possible, the Bank should consider terminating the contract with such international money transfer systems.

2.6.10. If the bank provides services to both the sending and receiving parties for money transfers, the Internal Control Service shall assume the following responsibilities:

- take into account all information received from both the sending party and the receiving party in order to determine whether a suspicious transaction report should be filed;
- forward a suspicious transaction report to the competent authorities in any country with which the suspicious money transfer is associated, and provide relevant information about the money transfer.

III. PROCEDURES FOR OPERATIONS MONITORING

3.1. Criteria and signs of doubtful and suspicious transactions

3.1.1. The operation is recognized as doubtful if one of the following criteria and signs is evident:

1) the Bank has assigned a high level of risk to the transaction or the customer performing it;
2) a systematic return by a resident customer of the previously received amount in favor of a non-resident under a contract for the supply of goods (performance of work, provision of services);
3) submitted documents for the transaction raise doubts about its authenticity (reliability), and (or) information about the transaction, including about any of its parties, does not correspond to the data available to the Bank;
4) unusual behavior of the customer when submitting an application (instruction, request) to perform a transaction, for example: nervousness, uncertainty, aggression with simultaneous participation of persons directing the customer's actions, or his phone call to other persons for advice on an insignificant occasion;
5) the customer's unusual concerns about confidentiality issues or unreasonable refusal or unjustified delays in providing the customer with information about transaction requested by the Bank's employees;
6) impossibility of establishing the customer's partners in the operation;
7) the operation does not have a clear economic meaning and does not correspond to the nature and type of the customer's activity;
8) an unreasonable increase in the turnover of funds on the customer's account that is not related to the nature of its activities and (or) occurred after more than a three-month period of low activity or absence of signs of activity on the accounts of such customer;
9) unreasonable and (or) early termination of business relations by the customer, accompanied by withdrawal or transfer of all funds to other commercial banks;
10) immediate termination of business relations by the customer after justified application by the commercial bank of the measures provided for by these Regulations;

11) a clear discrepancy between the operations carried out by the customer with the participation of the Bank and generally accepted practice of performing operations;
12) unreasonable splitting of the amounts of similar operations performed by the customer for a total amount equal to or exceeding 500 times the Reference Calculation Value on the day of operation;
13) the settlement procedure contains non-standard or unusually complex schemes that differ from usual activities of the customer;
14) exchange of banknotes of one denomination for banknotes of another denomination by an individual for an amount equal to or greater than 500 times the minimum wage established on the day of exchange;
15) deposit by an individual in cash in the amount equal to or exceeding 500 times the Reference Calculation Value on the day of operation, to the bank account of a legal entity or an individual entrepreneur as loans, financial assistance, contribution to the authorized capital (fund) or working capital for the purpose of replenishment;
16) transfer from the accounts of legal entities or individual entrepreneurs of funds in an amount equal to or greater than 1000 times the Reference Calculation Value on the day of operation, as financial assistance or a loan; transfer from the accounts of legal entities or individual entrepreneurs of funds in an amount equal to or greater than 500 times the minimum wage on the day of operation, as financial assistance or a loan;
17) transfer from the accounts of legal entities and / or individual entrepreneurs in favor of individuals of funds in an amount equal to or exceeding 1000 times the Reference Calculation Value on the day of transaction, as dividends or profits;
18) withdrawal of cash from the account of an individual in the amount equal to or exceeding 500 times the Reference Calculation Value on the day of transaction;
19) carrying out transactions (payment or cash withdrawal) from five or more international payment cards within one day at the terminal of one counterparty, when the amount of transactions with each card is equal to or exceeds 25 times the Reference Calculation Value;
20) transfer of funds, which amount is equal to or exceeds 500 times the Reference Calculation Value, outside the Republic of Uzbekistan to the beneficiary's account opened with a bank whose location is different from the beneficiary's place of registration.
21) transfer of funds by an individual in the name of another individual, which amount is equal to or exceeds 1000 times the Reference Calculation Value on the day of operation.
22) making payments in an amount equal to or exceeding 1,000 times the Reference Calculation Value established on the transaction date from plastic cards issued by the Bank or from plastic cards issued by another bank through a terminal installed by the Bank.

3.1.2. An operation is considered suspicious if one of the following criteria and signs is evident:

1) one of the parties to the operation is a person who permanently resides, resides or is registered in a state that does not participate in international cooperation in the field of combating money laundering and financing of terrorism;
2) receipt of funds sent from abroad or sending abroad by individuals (including several individuals in the name of one counterparty) in foreign currency, including through money transfer systems, for a total amount equal to or exceeding 500 times the Reference Calculation Value, at a time or repeatedly within a period not exceeding 1 month;
3) sale or purchase, as well as withdrawal from international payment cards by individuals and / or individual entrepreneurs of funds in foreign currency in an amount equal to or exceeding 500 times the Reference Calculation Value, at a time or repeatedly within a period not exceeding 1 month ;
4) transfer of funds outside the Republic of Uzbekistan to an account opened for an anonymous owner, and receipt of funds to the Republic of Uzbekistan from an account opened for an anonymous owner or in the absence of information about the sender;

5) transfer of funds outside the Republic of Uzbekistan to the beneficiary's account opened with a bank registered in an offshore zone that differs from the beneficiary's place of registration;
6) transfer of funds outside the Republic of Uzbekistan to accounts or in favor of persons permanently residing or registered in offshore zones, or received in the Republic of Uzbekistan from the accounts of such persons at a time or repeatedly within 30 days, for a total amount equal to or exceeding 500 times the Reference Calculation Value established on the day of the last transfer (receipt);
7) transactions with non-resident customers, information about the founders of which is not available and it is impossible to obtain it by all available methods;
8) a transaction related to the use of funds or other property to which access has been granted, including an attempt to conduct it;
9) other operations that do not have the criteria and signs provided for in this paragraph, established by these Regulations, in respect of which the commercial bank has suspicions of involvement in money laundering and (or) financing of terrorism.
10) transfer of funds by a non-resident to a resident as grants, financial assistance, loans or gratuitous assistance;
11) sending and receiving funds through international money transfer systems by citizens of the Republic of Uzbekistan located in areas with increased terrorist activity (the list of countries and territories is provided by the Department);
12) transactions of persons who are on the interstate wanted list for committing a crime of a terrorist nature (the list of persons is provided by the Department);
13) cash turnover of the legal entity - customer is equal to or exceeds 20,000 times the Reference Calculation Value within a period not exceeding 3 months from the date of creation of such legal entity, and is carried out for purposes that do not correspond to the nature of its activities;
14) purchase by individuals of coins, bullions of the Central Bank from precious metals for an amount equal to or exceeding 500 times the Reference Calculation Value, at a time or repeatedly within a period not exceeding 1 month.
15) Suspicious transactions, which decision to include it in the category of transactions is subject to notification by the Internal Control Service.

3.2. Identification of Dubious and Suspicious Transactions

3.2.1. Study of the customer’s activities shall be carried out by systematic verification and control of its operations.

Verification of customer transactions shall consist of current and subsequent verifications.

The current verification of the customer's operations in the Bank and its branches shall be carried out by divisions that carry out and control its operations in the following stages specified in section III "Instructions on the organization of accounting and accounting work in banks of the Republic of Uzbekistan" (registered on July 11, 2008 with the Ministry of Justice under No. 1834):

a) primary control;
b) current control;
c) final control.

Operations in the Bank's divisions must be organized based on this principle of three-stage control. At each stage of control, the relevant employees, along with monitoring the correct execution of the document, should pay attention to the essence of the operation, its connection or not with the type of customer's activity.

3.2.2. The information obtained in the course of identification, as well as the assigned level of risk of working with a customer, are the basis for monitoring transactions carried out (performed) by customers, carried out in order to make sure that such transactions correspond to the main areas of activity of the customer, and study, if necessary, sources of funds.

3.2.3. The current verification of customer transactions shall be carried out by the relevant employees of the Bank who directly serve customers (responsible executives, cashiers,

plastic card specialists, lending specialists, etc.), who, upon identification of transactions that have signs of suspicious and (or) doubtful transactions, shall immediately report in writing on such operations to his immediate supervisor and employees of the Internal Control Service, specifying the relevant criteria and signs specified in Annex No. 7 to these Regulations. When individuals carry out suspicious transactions, a copy of the document that served as the basis for the transaction shall be provided along with the report on the transaction.

If it is not possible to express the details of a suspicious transaction in the form specified in Annex No. 7 to these Regulations, the responsible employees directly serving customers can send a message on a suspicious transaction in a form convenient for them. In addition, it can be transmitted in one message for identical operations (for example, operations carried out from the customer terminal, etc.) or in the form of a table, with an attachment to the message.

Subsequent verification of customer transactions shall be carried out by employees of the Branch Internal Control Service by analyzing the customer's transactions made in the previous period in order to identify doubtful and suspicious transactions that are not detected at the current verification stage.

3.2.4. When transactions are identified that have signs of doubtful and (or) suspicious transactions, employees of a commercial bank directly serving customers, on behalf of the Internal Control Service, if necessary, contact the customer for additional information about the operation being carried out.

3.2.5. Communication with customers shall be carried out by employees of the division directly serving customers. In addition, responsible employees of the Internal Control Service can obtain additional information necessary for the proper study of the customer through employees directly serving customers.

3.2.6. Employees of the Internal Control Service shall examine details of the customer and transaction, enter the relevant information in a special register of the Internal Control Service in the form given in Annex No. 8, in the “Messages” file in the form of a password-protected spreadsheet in the form given in Annex No. 14, and in the customer's questionnaire, and in addition, if there are sufficient grounds, send a proposal to the Manager of the Internal Control Service to classify dubious transaction as suspicious.

3.2.7. Suspicious transaction notifications provided by responsible employees shall be registered in chronological order in a special electronic folder “Messages” by employees of the Internal Control Service of the branch and sent daily to the Head Office to the Compliance Control Department by “Lotus Notes” mail with a protected password.

An employee of the Compliance Control Department of the parent bank shall daily collect data on suspicious transactions from all branches into a single electronic file "Message-9055" and analyze suspicious transactions with the Manager of the Compliance Control Department.

3.2.8. In the event of reasonable suspicions, the Manager of Internal Control Service shall make a written decision to recognize the customer's transaction as suspicious and notify the bank's management about it.

In some cases, based on the level of risk of suspicious transactions, it may be allowed to immediately classify it as suspicious based on a written instruction (order) of the Bank's management.

3.2.9. Recognition of transactions as suspicious shall be carried out based on a comprehensive analysis using the criteria and signs of suspicious transactions determined by these Regulations in each individual case.

3.2.10. Recognition of transactions as suspicious in each case shall be based on a comprehensive analysis using the criteria and signs of suspicious transactions established by these Regulations.

After the customer's transaction is recognized as suspicious, the Internal Control Service must take the following measures:

- submit a suspicious transaction report to the Department;
- obtain additional information about the customer;
- reconsider the risk level of the customer;
- strengthen monitoring of customer's operations;
- make a proposal to the Chairman of the Management board of a commercial bank to terminate the contractual relationship with the customer in accordance with the law and the agreement executed with him.

3.2.11. A suspicious transaction report shall be transmitted by the Internal Control Service to the Department no later than one business day from the date the suspicious transaction is detected, in accordance with the requirements of Annex No.1 "Regulations on the procedure for providing information related to combating money laundering, financing of terrorism and financing proliferation of weapons of mass destruction" approved by the Resolution of the Cabinet of Ministers of the Republic of Uzbekistan No. 402 dated June 29, 2021.

3.3. Preparing suspicious transaction reports and forwarding them to the Department

3.3.1. If transactions are detected that meet the criteria and signs of suspiciousness provided for in paragraphs 1-9 Clause 3.1.2 to these Regulations, notifications shall be sent by employees of the Branch Internal Control Service no later than the day when they are detected to the Head Office by "Lotus Notes» mail in the form of a generated file using cryptographic protection through a special program, as well as in the form of a password-protected spreadsheet given in Annex No.14. The Internal Control Service at the Head Office shall submit reports on such suspicious transactions to the Department no later than the next working day, without attached analysis.

3.3.2. When transactions are identified that meet the criteria and signs of doubtfulness provided for in clause 4.1.1 to these Regulations, reports shall be sent by employees of the Branch Internal Control Service to the Head Bank by Lotus Notes mail in the form of a password-protected spreadsheet given in Annex No. 14.

Suspicious transactions received from branches shall be collected and analyzed, a list of transactions recognized as suspicious among them shall be sent to each branch by Lotus Notes mail in the form of a password-protected spreadsheet. Employees of the Branch Internal Control Service shall, no later than the day the list is received, send information about suspicious transactions to the Head Office by Lotus Notes mail in the form of a generated file using cryptographic protection through a special program, as well as in the form of a password-protected spreadsheet given in Annex No. 14.

3.3.3. Information on suspicious transactions filled in by employees of the Branch Internal Control Service shall be filed in the Moneyoper complex of automated software for filing, processing and transmitting information. Information and details must be entered carefully and correctly. Files with electronic messages sent to the Head Office must be stored in a separate folder.

Files received from branches by an employee of the Branch Internal Control Service shall be stored separately for each branch in the "Messages/Incoming" folder open for messages. These received files shall be opened through Moneyoper program, checked and corrected if there are errors and shortcomings. The messages shall be then re-stored in the "Messages/Incoming" folder as an electronic document, cryptographically protected and electronically transmitted, authenticated with an electronic digital signature in accordance with the law and sent to the Department through a special secure connection using Lotus Notes mail.

3.3.4. If messages are not sent to the Department in the form of electronic documents through a special secure connection, they shall be sent to the Department through electronic information media (floppy disk, CD and other memory installations), delivered by courier or by special postal service, with the exception of cases of a threat to the confidentiality

of the document.

3.3.5. If it is not possible to send messages in the form of an electronic document, they are provided by personal delivery or by means of a special targeted postal service on paper, in compliance with the requirements of the procedure excluding violation of the confidentiality of the document.

When messages are provided by courier or through special mail, the date of its submission shall be the date of its delivery by courier or transfer in accordance with the established procedure to special mail.

3.3.6. Information about each message shall be recorded in a special log.

The Internal Control Service shall daily generate information in paper form in the form of a table about the messages sent to the Department, indicating all the information from the electronic message. This table must be endorsed by the executive and approved by the Manager of the Internal Control Service.

When forming such tables, it is not required to transfer an electronic message to paper. The message sent to the Department, when transferred from electronic to paper, shall be certified by signature of the Manager of the Internal Control Service.

In case of absence of the Manager of the Internal Control Service, the table of transmitted messages and (or) a paper copy of the message shall be signed by his deputy or a responsible officer based on the authority granted to him in writing by the Chairman of the Management Board of the Bank.

3.3.7. All messages sent to the Department and information in tabular form about the messages sent must be stored directly by the Manager of the Internal Control Service in a specially equipped room or in a fireproof and sealed safe.

3.3.8. In addition, the Internal Control Service must immediately inform the Department of each information confirming the suspicion of the relevant transaction or excluding its suspicion.

3.3.9. If the message is delivered in an incorrect form or not delivered in full, as well as in the absence of an electronic digital signature (seal of the Bank, signatures of responsible persons or other required details), the Department shall, on the date of receipt of the message, send a request to resend the message, subject to confidentiality requirements and an accurate indication of the shortcomings.

After receiving a message of such content from the Department, the Internal Control Service shall take measures to correct the deficiencies specified in the request, and within one day from the receipt of the request shall resend the corrected message to the Department.

3.3.10. If the Bank has provided the Department with improper incorrect information about the operation, the Bank shall send a written request to the Department to consider the submitted information invalid.

The Bank's message must indicate the reasons for considering the information invalid, as well as information allowing to identify incorrectly provided information (number and date of the message, method of provision, transaction amount, currency and date of the transaction).

3.3.11. The Department has the right to send written requests regarding sent messages to the Bank requesting additional information and copies of duly certified documents:

- if there is a need to check the accuracy of received messages;
- as part of the fulfillment of obligations under international treaties of the Republic of Uzbekistan related to money laundering and financing of terrorism.

After receiving such requests, the Bank, within 3 working days, at the request of the Department, shall provide certified copies of the requested information by personal delivery or through special mail.

In turn, the Department may determine other terms for the provision of information, based on its scope and characteristics.

3.4. Measures taken to ensure the completeness of information on international money transfers, as well as in case of detection of money transfers in foreign currency, for which the required data are missing

3.4.1. The relevant departments of the Bank must take the necessary measures to ensure the completeness and reliability of the information required about the recipient and (or) sender of all international transfers (payments).

International transfers (payments) are operations related to a customer (or the Bank) counterparty (sender or recipient), which is an individual or legal entity, or the funds of its bank located in a foreign country.

3.4.2. When accepting a payment document for an international payment from a Bank customer that is a legal entity, an employee of the relevant department must pay attention to the name, address of the sender of money, the purpose of payment, as well as the name, country, address, bank (name, SWIFT code, country) of the recipient.

3.4.3. Upon receipt of funds for international payments to a Bank customer that is a legal entity, the appropriate employee of the Foreign Exchange Accounting Department, who performs foreign exchange control of legal entities, shall carefully check the document (SWIFT notice) that served as the basis for posting funds, and also pay attention to the presence and correct reflection in beneficiary's name, name, country, bank address (name, SWIFT code, country) of the sender and the purpose of payment.

3.4.4. In the case of full and correct reflection of the required information, the funds shall be credited to the customer's account.

3.4.5. In case of incomplete and incorrect reflection of the required information, the Foreign Exchange Accounting Department:

- if the name of the recipient or sender is not indicated, shall take measures to send a request to the non-resident bank to credit funds to the transit account and identify incomplete and incorrectly specified information, and also notify the Internal Control Service in accordance with the established procedure on the same day;
- if the name of the recipient and the sender is fully indicated, but one of the other required information is not specified (name, address, country of the sender, subject of payment), shall take measures to send a request to the non-resident bank to credit funds to the transit account and identify incomplete and incorrectly specified information.

3.4.6. In order to organize and control international money transfers of individuals, Money Circulation and Retail Operations Department must keep records of the divisions providing such services (departments, mini-banks, retail operations centers) and employees of such divisions.

Prior to execution of money transfer operations, employees of divisions providing such services shall properly verify customers - individuals.

3.4.7. Responsible employees of departments making international money transfers must ensure that the transfer is accompanied by accurate information about the customer sender (full name (if any); series and number of an identity document (passport or a document replacing it); if account is used during operation, then its number or a unique transaction code; sender's address or state identification number or identification number of the customer or, for individuals, date and place of birth), and about the recipient (full name (if any); account number, if in the process transaction used the customer's account or a unique transaction number).

3.4.8. Responsible employees of departments that carry out international money transfers on international money transfers to incoming customers - individuals, in the process of checking the completeness of information on such transfers, must:

- if at least one of the basic information is not indicated, that is, last name, first name,

patronymic (if any) or the country of the sender, the money transfer is not paid to the customer, and on the same day the immediate supervisor and the Internal Control Service shall be informed about this operation. For payments received from the sender in non-resident banks, a report shall be sent to the Monetary Circulation and Retail Operations Department. In turn, the Money Circulation and Retail Operations Department shall take measures to identify unspecified information (send appropriate requests to the international money transfer system or to a non-resident bank);

- if the surname, name, patronymic (if any) and country of the sender are indicated, but one of the other information is not indicated, a report shall be made to the Monetary Circulation and Retail Operations Department. In turn, the Money Circulation and Retail Operations Department shall take measures to identify unspecified information (send appropriate requests to the international money transfer system or to a non-resident bank).

3.4.9. In order to exercise effective control over the transactions of customers and promptly obtain information on them, the Foreign Economic Affairs Department and the Monetary Circulation and Retail Operations Department must keep records of all international money transfers.

Information on all international money transfers (payments) of legal entities and individuals should be maintained in the form of a spreadsheet and make it possible, if necessary, to obtain the necessary information, as well as group and filter by indicators (country, amount, type of payment, etc.).

3.4.10. The Internal Control Department, the Foreign Economic Affairs Department and the Money Circulation and Retail Operations Department shall generate a database of all international money transfers (payments) of legal entities and individuals and use it to analyze, control and report on customers transactions.

3.5. Provision of information on violations of the law by employees of the internal control to the Manager of the Internal Control Service

3.5.1. The Manager of the Internal Control Service, within the scope of his powers, must take the necessary measures for the proper organization and provision of activities in the Bank to combat money laundering and financing of terrorism.

The Manager of the Internal Control Service, in order to control the organization in the branches of the internal control system, must be in constant contact with the internal control employees assigned to it.

3.5.2. The internal control officers assigned to the branches of the Bank, assessing the degree of implementation of the internal control system in the branches, must respond appropriately to improve it or eliminate the deficiencies, in particular, to inform the Manager of the Internal Control Service, who is the immediate supervisor.

Employees of internal control in the course of performing their functions shall pay special attention to:

- correct establishment of customer due diligence by employees of the relevant departments, in particular, timely and complete entry of information on their identification into electronic questionnaires of customers;
- taking appropriate measures by employees of relevant departments in the process of customer due diligence to identify public officials;
- timely identification of suspicious transactions by employees of the relevant departments and reporting to employees of internal control;
- timely submission of information on suspicious transactions to the Head Office;
- reporting to the management on the state of internal control in the bank, including making proposals for submitting reports on doubtful and suspicious transactions and improving the internal control system;
- correct maintenance of documents in the Bank on internal control related to combating money laundering and financing of terrorism.

3.5.3. In case of deficiencies in the performance of these tasks (identification of customers,

filling out electronic questionnaires, updating identification data, identifying and reporting questionable and suspicious transactions, maintaining spreadsheets on international payments) by the employees of the branch involved in performing functions under the internal control system, an employee of the Internal Control Service shall address the Branch Manager and Manager of the Internal Control Service about this with a request to take appropriate measures against the guilty employees.

If employees of the branch fail to comply with the requirements established by these internal Regulations, make gross mistakes and repeat shortcomings, the Manager of the Internal Control Service shall apply in writing to the Chairman of the Management Board with a request to take action against the relevant employees.

3.5.4. Employees of internal control must be provided with the necessary hardware and software to perform their functions. The internal control staff of each branch should be provided with a separate transmitting and receiving Lotus Notes address program for generating, sending to the Department and receiving notices in the form of an electronic file with cryptographic protection.

3.5.5. Employees of the Branch Internal Control shall send information about doubtful and suspicious transactions to the Manager of the Internal Control Service of the Head Office in the form of a table file generated by Excel program with a password. Notifications of transactions that meet the suspicious criteria shall be also sent as an electronic file with cryptographic protection.

If necessary, the employees of the internal control of the Head Office may request additional information regarding the customer or the operations carried out by it. In such cases, branch employees take measures to ensure the confidentiality of the information delivery.

IV. PROCEDURE FOR IDENTIFYING, ASSESSING, MANAGING AND DOCUMENTING THE RISK LEVEL

4.1. Identification of the risk level of customers, keeping records and monitoring of customers belonging to the highest risk level

4.1.1. The Internal Control Service must respond appropriately to identify, assess, monitor, manage and reduce the risk level.

The Internal Control Service must determine the overall level of risk, the required level of its reduction and implement an appropriate program of measures depending on the types and level of risks.

The Internal Control Service shall systematically, at least once a year, study, analyze and identify possible risks of money laundering, financing of terrorism and financing proliferation of weapons of mass destruction, and document the study results.

The Internal Control Service must determine the overall risk level, the required level of its reduction and implement an appropriate program of measures depending on the types and risk levels.

The measures applied should allow decisions to be made on the implementation of enhanced or simplified measures to control the identified risks and effective allocation of resources.

The risk level shall be identified and assessed by a responsible officer based on the information provided by the customer, taking into account the types of activities and transactions performed by the customer, the criteria established by these Regulations, the results of customer due diligence, risk factors (by types and activities of customers, banking facilities and services, supply chains, geographic regions and others), including on the basis of the study and analysis of information provided by the customer.

Results of the risk assessment must be submitted to the Central Bank of the Republic of Uzbekistan.

4.1.2. An employee of the Internal Control Service, according to the information obtained as a result of due diligence by employees of departments (corporate customer service department, retail operations and plastic cards department, etc.), directly serving customers, in accordance with the criteria defined in these Regulations, shall determine the risk level for customers based on the issued information on compliance with the high risk category.

4.1.3. In order to timely and correctly classify customers as a high-risk category, employees of the Internal Control Service no later than the business day following the day of customer due diligence (opening an account, performing a one-time operation), based on the information reflected in their electronic questionnaires, determine in the electronic questionnaire classifying or not classifying them as high-risk.

Employees of the Internal Control Service, having checked the documents (legal folders) reflecting the identification information of legal entities and individual entrepreneurs, check the completeness and correct entry of this information into electronic questionnaires.

If necessary, employees of the Internal Control Service may also request primary documents of individuals (application, contract, copy of an identity document, etc.).

4.1.4. If the customer's electronic questionnaire is not generated, an employee of the Internal Control Service shall inform the Manager of the department responsible for filling out the electronic questionnaire and require the electronic questionnaire to be completed in a timely manner.

After generation of the customer’s electronic questionnaire, if the customer, according to the criteria established by these Regulations, belongs to the high risk level, the employee shall put a corresponding mark in his electronic questionnaire.

4.1.5. After an employee of the Internal Control Service puts a mark in the customer’s electronic questionnaire that he is classified as a high-risk category, he shall print his questionnaire in paper form and, in order to confirm the information included in the electronic questionnaire, submit it to the Chief Accountant, or to in his absence, to his deputy or responsible officer.

Questionnaires submitted in paper form must be immediately reviewed, and in the absence of errors, signed and returned back.

4.1.6. Employees of the Internal Control Service shall maintain daily electronic lists of customers who do not have electronic questionnaires and classified as high-risk. The electronic list of customers classified as a high-risk category, in addition to information about customers, should reflect the criterion by which it is classified as a high-risk category, the date of commencement of business (for legal entities and individual entrepreneurs), what types of remote services he uses or not in use, date of categorization as high risk. The automated banking system should provide the ability to obtain information about customers classified as high-risk.

In case of repeated cases of untimely completion of electronic questionnaires, an employee of the Internal Control Service shall address this to the Branch Manager and Manager of the Internal Control Service, specifying factors hindering the effective operation of the internal control system, as well as with a request to take appropriate measures against the employees guilty of this.

4.1.7. If a customer or a transaction performed by the customer is classified as a high risk level, the Internal Control Service shall constantly monitor transactions carried out by this customer.

4.1.8. Depending on the change in the category of operations carried out by the customer, the Internal Control Service, if necessary, must review the risk level for working with it.

When an employee of the Internal Control Service excludes a customer from the high-risk category, he shall make a corresponding change in his electronic questionnaire and

the electronic list of customers classified as high-risk, and remove his questionnaire in paper form from the folder of questionnaires for customers classified as high-level risk.

4.2. Criteria for high-risk customers and transactions

4.2.1. The Internal Control Service shall classify customers as high-risk if they initially meet the following criteria, in respect of which the relevant departments should pay special attention to:

a) persons on the List or entities owned or controlled by a person on the List, or persons directly or indirectly owning or controlling an entity on the List;
b) persons permanently residing, staying or registered in a state not participating in international cooperation in the field of combating money laundering and financing of terrorism;
c) representative offices of foreign companies and non-residents - individuals of the Republic of Uzbekistan;
d) persons permanently residing, located or registered in an offshore zone;
e) residents and non-residents with accounts in offshore zones;
f) organizations and individual entrepreneurs, the actual location of which does not correspond to the information specified in the constituent or registration documents;
g) organizations, the beneficial owner of which is the person specified in paragraphs "a" and "b" of this clause;
h) customers who carry out suspicious or doubtful transactions on a systematic basis (for example, within 3 consecutive months);
i) customers using software systems that exclude the possibility of customer due diligence;
j) public officials, members of their families and persons close to public officials;
k) persons included in the current lists of the UN (based on Security Council Resolutions) and the Office of Foreign Assets Control of the US Department of the Treasury (OFAC SDN List) and known to the Bank.

4.2.2. The Bank shall classify high-risk transactions that meet the following criteria and in respect of which it must pay special attention:

a) transactions, which participants are the persons specified in paragraphs “a”, “b”, “h”, “l” and “m” Clause 3.2.1 of these Regulations;
b) transactions carried out through accounts opened in offshore zones;
c) transactions with precious metals, precious stones, as well as jewelry containing precious metals and precious stones, with the exception of such transactions carried out by commercial banks themselves;
d) transactions related to money transfers, in which information about the sender (last name, first name, patronymic of individuals, full name of legal entities, location (postal address) and account number of the sender) is not specified in full;
e) transactions with banks of states that do not participate in international cooperation in the field of combating money laundering and financing of terrorism, and transactions with parties registered in these states;
f) transactions which participants are the persons specified in paragraphs "k", "l" Clause 3.2 of these Regulations.

4.3. Measures aimed at preventing the use of technological advances for the purpose of money laundering and (or) financing of terrorism

4.3.1. The Bank must take measures aimed at preventing the use of technological advances for money laundering and (or) financing of terrorism. To this end, the relevant divisions of the Bank must determine and assess the levels of risk that may arise in connection with;

- development of new types of services and new business practices;
- using new or developing technologies for both new and existing services.

4.3.2. This risk assessment should be carried out prior to the launch of new services, business practices, or the use of new or emerging technologies. At the same time, this risk should be determined and assessed by the Bank's subdivision directly implementing new types

of services (new technology), together with the Internal Control Service.

This division of the Bank and the Internal Control Service must respond appropriately to monitor and mitigate these risks.

4.3.3. A unit that initiates the introduction into practice of new or development of existing types of services and new work operations, using technological advances, shall submit a proposal to this effect to the Branch Manager where it operates. The Branch Manager shall consider this proposal and, if further consideration is appropriate, shall submit it to the relevant department (departments) that control and coordinate this type of service or work operation.

The relevant management(s) or the offeror himself, in addition to analyzing the convenience and efficiencies arising from the introduction of new or existing types of services and new work operations, using technological advances, must identify and assess the possible risk level.

The relevant department (departments), having assessed the risk level, shall provide the Internal Control Service with a proposal for a new type of service or working practice, including with detailed coverage of technical aspects, to review and assess the level of risk, as well as to make proposals for reducing this risk.

4.3.4. The Internal Control Service must study in detail all features of the proposal associated with the introduction of a new type of service or work operation. If necessary, the Internal Control Service has the right to request assistance from other divisions of the Bank (Information Technologies Department, Legal Department, etc.).

The Internal Control Service, having studied and assessed the risks, shall provide the Management Board of the Bank with a written opinion specifying the possible levels of risks, as well as appropriate measures to monitor and reduce these risks.

4.3.5. Introduction of new types of services and new work operations, using technological advances, shall be carried out based on a decision of the Management Board of the Bank.

4.3.6. In order to reduce the risk, the relevant divisions of the Bank providing remote services, shall:

- in contracts executed with customers for the provision of remote services, provide for measures (suspension of the provision of this service to the customer until the customer explains in writing the legality of the operations performed; refusal to provide this service) taken in case of detection of suspicious transactions carried out by the customer using such services;
- study the customer at the location (postal address) or the address specified in the contract for the provision of remote services, including study the process of carrying out the transaction directly by the person specified in the contract for the provision of remote services, if there are doubts about conducting suspicious transactions with use of remote services;
- suspend the provision of remote services, with the use of which suspicious transactions are carried out, for the period specified in the contract for the provision of this service;
- terminate the contract for the provision of remote services in the prescribed manner if there are reasonable suspicions that such services are used for the purpose of money laundering and financing terrorism.

4.3.7. When studying a customer using remote services, at his location (postal address) or the address specified in the remote services agreement, the relevant divisions of the Bank should pay special attention to the customer’s compliance with the requirements of the Regulation for non-cash payments in the Republic of Uzbekistan (reg. No. 2465 dated June 3, 2013) (Collected Legislation of the Republic of Uzbekistan, 2013, No. 23, Art. 309), including execution of settlement documents, its certification by the signature of authorized persons (Manager, Chief Accountant), making transfers on these documents only after confirmation electronic digital signature by a person directly entitled to an

electronic signature and storage of these documents.

4.3.8. In order to provide high-quality and modern services by the Bank's divisions, increase the productivity of employees, as well as improve the performance of the internal control system, the relevant divisions should take measures to study and implement modern technologies, facilitate work processes, improve existing software, introduce sound and useful management types of reports.

4.3.9. The Internal Control Service, in the performance of its duties, may study the software used by other units and the reports prepared by them, as well as make proposals to the Bank's management to adapt them to modern requirements. In addition, in some cases, if the need arises, it has the right to request from units to prepare reports related to their activities.

4.3.10. The database resulting from customer due diligence should be able to quickly and conveniently generate useful reports from this data, in particular it should meet the following requirements:

- print in paper form of customer questionnaires;
- search and grouping by several indicators (name, country, type of activity, address, etc.) among all categories of customers;
- automatic control at the maximum level of assigning a certain level of risk to customers based on existing criteria;
- obtain information on customers and their real owners in the registered and residing in offshore zones and states that do not participate in international cooperation in the field of combating money laundering and financing of terrorism, etc.

4.3.11. The Information Technology Department shall take appropriate measures to systematically improve the information technologies used in the Bank, in particular the automated banking system and other software. The Internal Control Service may contact this unit on such matters.

V. CUSTOMER DIGITAL IDENTIFICATION

5.1. General rules for customer digital identification

5.1.1. Prior to the introduction of a customer digital identification system, measures will be taken to study, analyze, identify, evaluate, monitor, manage, document and reduce the potential risk of money laundering, terrorist financing and proliferation of weapons of mass destruction.

The Internal Control Service analyzes and assesses risks, submits a written report to the Management Board of the Bank indicating possible levels of risks and appropriate measures to monitor and reduce them.

5.1.2. When digitally identifying customers, the relevant departments of the bank must take the following information security measures:

- the necessary legal, organizational and technical measures to protect the customer's identification data;
- ensuring the reliability and accuracy of identification information;
- take measures against forgery, unauthorized alteration and disclosure of identification information;
- control over the storage and use of identification data;
- take measures to reduce and control operational risks associated with information security in the provision of payment services, including security in the digital identification of customers;
- application of procedures for multi-factor authentication of the customer when using banking services (communicating by mobile phone or sending SMS or e-mail, as well as additional verification and confirmation of the customer's identity through social networks);

– apply the necessary requirements in accordance with other legislation in this area.

5.2. Customer Digital identification

5.2.1. Digital identification shall apply to citizens of the Republic of Uzbekistan, foreign citizens and stateless persons permanently or temporarily residing in the territory of the Republic of Uzbekistan.

5.2.2. The following methods shall be used for customers digital identification:

- customer verification and identification by the responsible employee based on the information provided by the customer;
- real-time customer verification and identification without the human factor by information systems.

5.2.3. When verifying and identifying a customer based on the information provided by the customer, the system shall:

– receive from the customer photographs of an identity document (biometric passport or identification ID-card or driver's license of a new type) with relevant information in accordance with the requirements of internal control Regulations;
– accept a photo and (or) video of the customer in accordance with the established requirements;
– compare with the data of individuals and legal entities by sending a request to the central databases of the Electronic Government system (hereinafter referred to as the central database);
– compare the photo in the identity document with the photo and (or) video taken in accordance with these Regulations, as well as with the photo (if any) placed in the central database;
– check the mobile phone number used to communicate with the customer by a method that allows to determine whether it is used by the customer (connecting a mobile phone, sending SMS);
– in accordance with internal control Regulations, check whether the customer belong to the high-risk category.
– a responsible employee shall establish an online video conference session with the customer and check that the received documents belong to him.

5.2.4. Real-time customer verification and identification without the human factor by information systems:

a) the series and number of an identity document (biometric passport or identity card or a new driver's license) or the personal code and date of birth of an individual or all of this information and photograph in accordance with the Regulation on customer digital identification or real-time video capture;
b) send a request to the central database and receive the following personal information of the customer:
   - digital photography (if any);
   - personal identification number of an individual (TIN);
   - date of issue of the biometric passport or identity card, its validity period and place of issue;
   - surname, name, patronymic in the state language (in Latin);
   - information about gender, country of birth, place of birth, nationality, citizenship and place of permanent or temporary residence;
c) real-time photo taken from the customer or photo in video with a photo from the central base (if any)
   - compare automatically (without human factor);
d) check the mobile phone number used to communicate with the customer using a method to determine whether it is used by the customer (connecting a mobile phone, sending SMS);

e) compare the received data with the List in automatic mode (without taking into account the human factor) in accordance with the internal control Regulations.

5.2.5. The relevant divisions of the Bank shall ensure that the information systems used for customer digital identification or digital authentication comply with the requirements for the personal information of the customer (photo or video) received through them.

5.3. Use of digital identification

5.3.1. Digital identification can be used to provide the following services, subject to certain requirements:

- opening and managing electronic wallets;
- opening and managing a bank account, as well as a bankcard;
- cross-border money transfers using bankcards or electronic money systems;
- receive an online loan.

5.3.2. Strict restrictions are imposed on the following transactions with digitally identified customers, with an assessment of the risk level in accordance with internal control Regulations:

- maximum amount of one operation performed by the owner of electronic money;
- maximum amount of electronic money stored on one electronic device of the owner of electronic money;
- amount of transactions value made by the owner of electronic money during the calendar month;
- amount of transactions value made by the owner of the bank account (card) during the calendar month;
- number of transactions made by the owner of electronic money and (or) the owner of the bank account (card) during the calendar month;
- amount of online microcredit.

These restrictions are developed by the responsible departments of the bank in agreement with the Internal Control Service and approved by the Management Board of the Bank.

Other restrictions may be imposed on the customer digital identification and digital authentication of previously identified customers by the Internal Control Service, assessing the risk level of each customer's transactions.

5.3.3. If attempts by customers to circumvent established restrictions are detected, steps must be taken to terminate any practical business relationship with such a customer or to abandon his transactions.

5.3.4. Customers are not identified digitally in the following cases:

- if a transaction performed by the customer and (or) the customer is classified as high risk in accordance with the internal control Regulations;
- in case of doubts about the reliability of the information provided by the customer;
- if there is any doubt that the photo in the identity document corresponds to the photo and (or) video taken in accordance with the Regulation "Concerning the procedure for customers digital identification" and the photo (if any) posted in the central database;
- when the data received from the customer does not correspond to the data placed in the central database, or inability to verify compliance;
- non-compliance of the photo and (or) video recording with the requirements of the Regulation "Concerning the procedure for customers digital identification ";
- if there are doubts about money laundering, financing of terrorism and financing of the proliferation of weapons of mass destruction.

5.3.5. In case of digital identification, in case of partial or complete compliance of all customer identification data with the data of the Registered Person, measures shall be taken in accordance with Section VI of the Internal Control Regulations.

5.3.6. Filling in and maintaining the customer questionnaire based on the results of the customer digital identification shall be performed in accordance with the requirements established by the internal control Regulations.

5.3.7. In addition to the information required by the Internal Control Regulations for digitally identified customers, photos and/or videos taken from customers, documents indicating the exact date and time of verification and customer identification, as well as the results of data verification using a central database of customer questionnaires shall be stored together for five years in accordance with internal control Regulations.

VI. PROCEDURE FOR CONTROL OVER THE OPERATIONS OF PERSONS INCLUDED IN THE LIST

6.1. Measures to be taken when transactions involving persons included in the List are identified

6.1.1. When carrying out transactions, responsible employees of the relevant divisions of the Bank shall verify the identification information of participants in transactions with the List.

In the event that all identification data of the customer or one of the participants in the transaction completely matches the data of the person included in the List, the Bank shall immediately and without notice suspend this operation (with the exception of operations to include funds received on the account of a legal entity or individual) and (or) freeze cash or other property.

A full match means exact and unambiguous correspondence of the available identification data of a customer or one of the participants in the transaction to all relevant information contained in the List.

A transaction with cash or other property is also subject to suspension, and cash or other property to freezing, in cases where:

- one of its participants acts for or on behalf of a person included in the List;
- funds or other property used for the transaction is wholly or partly owned or controlled by a person included in the List;
- funds or other property received or acquired using funds or other property directly or indirectly owned or controlled by persons included in the List;
- a legal entity participating in a transaction is owned or controlled by an individual or legal entity included in the List.

6.1.2. When suspending a transaction and (or) freezing funds or other property of a person included in the List, the Internal Control Service shall send a notification of a suspicious transaction to the Department no later than one business day, indicating the value of the frozen property.

6.1.3. If during the establishment of relations or during the operation, the Bank's employees establish a complete match of all identification data of the customer or one of the participants in the transaction with the person included in the List, they must immediately and without notifying the customer inform the Internal Control Service about this. In turn, the Internal Control Service must take the following measures to:

- detailed identification of the customer identity, beneficial owner of the customer or one of the participants in the transaction, to the extent possible;
- identification of funds or other property related to the transaction subject to freezing in accordance with the requirements of the legislation and these Regulations;
- preparation and submission for signature of the bank's management of an order to suspend the operation, with the exception of operations for crediting funds received to the account of a legal entity or individual, and freezing funds or other property for such an operation;
- preparing and sending to the Department a report on a suspicious transaction related to cash or other property on the day the transaction is suspended;

- obtaining additional information about the customer (including the type of activity, size of assets, information available through open databases, etc.);
- determining the source of funds or the source of the financial condition of the customer, including by obtaining information from the customer;
- entering information about the operation in a special register.

Responsible employees of the Bank have the right to inform the person included in the List about the suspension of his operation and (or) freezing of funds or other property only after the implementation of the measures provided for in this clause.

6.1.4. In case of suspension of the operation, funds or other property are not provided at the request of the customer.

The customer's application must be registered in accordance with the form specified in Annex No. 10 in a separate register for registering applications of customers whose operations are suspended, and placed in a special folder until the operation is resumed.

In a separate register for registering applications of customers whose operations are suspended, information is recorded that allows you to identify the suspended operation as well as participants of such transaction.

6.1.5. The Bank shall resume the suspended operation and provide access to the frozen property in the manner prescribed by the Regulations on the procedure for suspending operations, freezing funds or other property, providing access to frozen property and resuming operations of persons included in the List of persons participating or suspected of participating in a terrorist activities or proliferation of weapons of mass destruction (registration No. 3327 dated October 19, 2021).

6.1.6. The Internal Control Service shall ensure that the List is updated within the ABS system of the Bank on a regular basis, with each update of the List, but at least once every three months, to monitor the existing database of customers and their beneficial owners in order to identify funds or other property of persons subject to freezing every time the List is updated, and also at least once every three months.

6.2. Resumption of transactions related to suspended funds or other property and unfreezing of property of persons included in the List. Forwarding to the Department of applications issued to unfreeze suspended funds or other property

6.2.1. An organization carrying out transactions with cash or other property shall resume the suspended operation and (or) unfreeze cash or other property on the day of receipt of the following information, but no later than the next business day:

- on the exclusion of a person from the List;
- Department notification confirming a "false activation".

6.2.2. The person included in the List or another participant in the transaction has the right to apply to the Bank to obtain access to the frozen property for the following purposes:

b) purchases of food, medicines and medical products, rent, mortgage, utility bills, medical services, taxes and fees, insurance payments, lawyers and legal advice services within average market prices, current payments and fees, related to the maintenance of bank accounts or the maintenance of property;
c) payment of extraordinary expenses;
d) provided for in UN Security Council resolutions 1718 (2006), 1737 (2006), 2231 (2015) and resolutions adopted in their development.

The application shall be accompanied by information on the purpose, amount and justification of the payment, what part of the frozen property is supposed to be used, the details and identification data of the recipient of funds or other property, the bank recipient of funds.

6.2.3. The Internal Control Service shall forward it to the Department no later than one working day after receiving the application.

The Department shall inform the Bank about the decision taken after implementing the measures prescribed by the legislation.

In turn, the Bank shall, on the same day of receipt of the message from the Department, but no later than the working day following the day of receipt, execute the decision of the Department and inform the customer about it.

6.2.4. An operation related to the use of funds or other property to which access has been granted, including an attempt to conduct it, shall be reported by the responsible officer to an employee of the Internal Control Service, and shall be recognized by the Internal Control Service as suspicious and shall be subject to notification to the Department in the manner prescribed by law.

6.3. Technical procedure for working with the SWIFT Transaction Screening Utility program to operate transactions involving persons on the Lists.

6.3.1. SWIFT Transaction Screening Utility shall check the compatibility of sender and recipient payments with selected international Listings.

6.3.2. The authority to timely approve or reject payments by senders and recipients in foreign currency using the SWIFT Transaction Screening Utility software shall be vested in employees of the Compliance Control Department (hereinafter referred to as employees) in accordance with the decision of the Chairman of the Management Board.

The title of administrator of the SWIFT Transaction Screening Utility software (supervisor) shall be assigned to the Manager of the Compliance Control Department, Manager of the Financial Monitoring System Development and Coordination Department, Manager of the Request Sanctions Lists Department (hereinafter referred to as the responsible employee).

6.3.3. The SWIFT Transaction Screening Utility software shall check the validity of blocked payments due to possible resemblance to persons on international lists and make an independent decision on whether to transfer this payment.

6.3.4. If the information about the sender and recipient of payments coincides with the persons included in the list, the personnel shall take measures, i.e. the exact correspondence of similar information shall be checked and additional information obtained from open sources shall be studied.

When the verification determines that the listed persons are fully eligible, the responsible officer will decide not to transfer the payment through the SWIFT Transaction Screening Utility software. Unsettled payments shall be returned by the Foreign Economic Relations Department to the customer's account in accordance with the Regulations of internal control or to the account of a foreign bank with the reason "DUE TO INTERNAL POLICY".

VII. REGISTRATION, STORAGE, ENSURING CONFIDENTIALITY OF INFORMATION AND DOCUMENTS OBTAINED AS A RESULT OF INTERNAL CONTROL

7.1. The Bank and its branches should bring into a unified system the execution and storage of internal control documents on combating money laundering and financing of terrorism.

7.2. To store internal control documents in the Bank and its branches, employees of the Internal Control Service shall maintain the following folders and registers:

1) questionnaires of customers who are individuals;
2) questionnaires of customers who are individual entrepreneurs;
3) questionnaires of customers - being legal entities;
4) documents collected for the establishment of correspondent relations and correspondent banks (only in the Head Office);
5) documents on establishing relations with international money transfer systems and their customer due diligence (only at the Headquarters);

6) reports of employees about suspicious transactions of customers;
7) reports submitted to the Department regarding suspicious transactions (only in the Head Office);
8) instructions of customers with suspended operations;
9) information related to the verification or analysis of the customer's operations;
10) information submitted to the management of the Bank;
11) correspondence with the management and other divisions of the Bank;
12) obligations of hired employees to familiarize themselves with the Regulations of internal control and comply with these Regulations;
13) a log of employees' messages about suspicious transactions of customers;
14) register of suspicious transactions reported to the Department (only at the Head Office);
15) register of customers' instructions with suspended operations;
16) decisions of the Manager Internal Control Service to transfer doubtful transactions to suspicious ones (only in the Head Office);
17) inquiries of the Department on customers;
18) a list of persons associated with terrorist activities provided by the Department;
19) a list of states submitted by the Department that are not participating in the field of combating money laundering and financing of terrorism.

In the collections listed above, the documents shall be bound in chronological order.

7.3. The procedure for taking appropriate measures to identify, assess, monitor, manage, reduce and document risks;

7.4. Documents related to customer due diligence, executed in full or in any part in a foreign language, must be requested by a non-bank credit institution, if necessary, with a translation into the state or Russian language.

7.5. In the event of doubts as to the authenticity of the submitted copies of documents or other need, the non-bank credit organization shall have the right to demand that the original documents be submitted for familiarization.

7.6. Information about the customer obtained during the customer due diligence shall be indicated in the customer’s questionnaire in accordance with Annex No. 3 to these Regulations.

7.7. Electronic questionnaires of individuals shall be filled in by employees of the relevant departments (savings, currency exchange, cash, credit, etc.), assigned with these tasks.

Responsible employees of the relevant department who perform customer due diligence during a one-time transaction, on the upper left side of the back side of copies of documents confirming the identity of customers, shall record the date and amount of the transaction, and chronologically file it into separate folders for each type of transaction (cash withdrawal from plastic cards of other banks, transfer of payments from plastic cards of other banks, transfer of payments through a transit account without opening a personal account for the customer, etc.). For transactions related to plastic cards, responsible employees can take a copy of the check received from the terminal without manually recording the date and amount of the transaction on the reverse side of the copy of the document.

In addition, responsible employees who carry out customer due diligence, according to the details subject to identification of one-time transactions of the customer, must daily enter electronically in the form specified in Annex No. 11, withdrawal operations through the cash terminal located in the Bank from plastic cards issued by other banks, according to the form specified in Annex No. 12, payments for goods and services made through the terminal located in the Bank from plastic cards issued by other banks, in the form specified in Annex No. 13, non-cash payments for goods and services made by individuals without opening a personal account

7.8. Electronic questionnaires of entrepreneurs and legal entities shall be filled in by employees of the Department for the provision of corporate services to legal entities.

7.9. The electronic customer questionnaire shall be filled in by the responsible employee who

identified the customer, or by the Manager of the department in which he works. In some cases (for example, if the employee who performed the identification does not have a computer, or the computer at which he works is not able to enter the database, etc.), the Branch Manager may entrust filling in the customer's electronic questionnaire to another employee. However, this task must be specified in the Job Description of the employee to whom it is assigned, or fixed by order.

7.10. When filling out electronic customer questionnaires – for individuals and legal entities, responsible employees must enter the relevant information about the customer into the software, as well as fully and correctly reflect it in the electronic questionnaire, in compliance with the requirements specified in Annex No. 6.

The information in the questionnaire must be filled in by employees in the prescribed manner as completely and legibly as possible. Incorrect or incomplete filling by an employee is not allowed, with the pursuit of personal interests with the customer.

Managers of the relevant departments must provide employees with the necessary primary documents to fill out the questionnaires, as well as take the necessary measures to ensure its complete safety.

7.11. Employees of the Internal Control Service, in order to study the correct reflection of information in the customer's questionnaire, have the right to request from the relevant employees legal folders, cards and samples of the signature and seal, copies of documents (passport or a document replacing it) confirming the identity of the person authorized to sign financial documents etc. These employees shall submit such documents in a timely manner when requested.

7.12. Questionnaires shall be filled out electronically for all customers (with the exception of customers for whom customer due diligence measures are not required) using special programs. Questionnaires shall be also filled out on paper for customers carrying out dubious and (or) suspicious transactions, and for customers classified as a high-risk category.

The customer's questionnaire, filled out in electronic form, when transferred to paper, shall be certified by signature of the Chief Accountant or, in the absence of the Chief Accountant, by his deputy or responsible officer.

7.13. Questionnaires filled out electronically shall be stored in an electronic database that allow employees of a commercial bank who identify the customer, as well as payment agents and payment subagents, to have online access in a constant mode to check information about the customer.

7.14. The customer questionnaire shall be stored for at least five years from the date of termination of the relationship with the customer.

7.15. As the information specified in the customer's questionnaire changes, as well as the nature of financial transactions carried out by it, the Internal Control Service shall, if necessary, revise the level of risk of working with it.

7.16. Information about transactions should be formatted in such a way that, if necessary, it is possible to restore the details of the transaction. The Internal Control Service and the Information Technology Department, together with the relevant departments, must take all necessary measures to provide access to high quality and prompt receipt of reports on transactions (international payments, letters of credit, money transfers, transactions through plastic cards, dubious and suspicious transactions, etc.).

7.17. The relevant divisions of the bank shall store information about transactions, as well as identification data and customer due diligence materials for the periods established by law, but not less than five years after the implementation of transactions or termination of business relations with customers.

7.18. Manager of the Internal Control Service, in order to formalize the measures taken, must provide all employees in the branches with special registers given in Annex No. 8.

A special register must be bound, numbered, indicating on its reverse side the number of pages, the date (year, month and day) of the beginning of the register, and certified by signature of the Manager Internal Control Service.

7.19. In order to restrict access to documents (correspondence with the Central Bank and the Department, including paper and electronic copies of messages submitted to the Department; paper and electronic customer questionnaires; registers, etc.) used in the activities of the Internal Control Service (responsible officer), such documents and its inventory must be stored directly by the Internal Control Service (responsible officer) in specially equipped premises or in a fireproof and sealed safe for the periods established by law, but not less than for five years.

After the expiration of the storage period, the documents shall be handed over in the prescribed manner to the archive of a commercial bank.

7.20. Electronic versions of documents must be archived by software, recorded on electronic media and stored by the Manager Internal Control Service, together with the inventory, in a fireproof and sealed safe. At the end of each month, the Internal Control Service shall archive and record on CD or DVD CDs the following electronic files:

e) Clients List (YYYY-MM) - in ascending order, the list of customers at the end of the quarter;
f) High-Risk (YYYY-MM) - in ascending order, the list of customers included in the high-risk category at the end of the quarter;
g) Terrorists-list (YYYY-MM) - in ascending order, the list of persons associated with terrorist activities provided by the Department at the end of the quarter;
h) Messages (YYYY-MM) - in ascending order from the beginning of the year, a list of messages on suspicious and suspicious transactions at the end of the quarter;
i) in the Incoming-messages and Outgoing-messages folders, respectively, messages received from branches and messages sent to the Department during the quarter shall be stored;
j) in the Reports folder (YYYY-MM) the reports submitted to the Central Bank shall be stored in ascending order on a monthly basis and from the beginning of the year for the past quarter;
k) in the Requests folder (YYYY-MM), requests for customers received during the quarter shall be stored separately in folders named in the format "YYYY-MM-DD_(method of receipt)_(number of persons)".

7.21. Bank employees shall limit access to information related to combating money laundering and financing of terrorism, including documents stored in the Bank's archives, ensure its non-proliferation and shall not inform legal entities and individuals about the provision of messages about their operations to the Department.

They ensure non-disclosure (or non-use for personal purposes or in the interests of third parties) of information obtained in the course of their internal control functions.

7.22. Disclosure of information, including from the questionnaire that constitutes the customer's identification data, to third parties shall be carried out in accordance with the law.

7.23. Information obtained as a result of customer due diligence and identification must be updated at least once a year in cases where the Bank assesses the risk of the customer's money laundering or financing of terrorism as high, in other cases at least once in three years and in the presence of changes in the information of the customer.

7.24. Customer due diligence information for a one-time transaction shall be updated at the next time transaction that requires to perform customer due diligence.

7.25. The Bank shall ensure that payment agents and payment subagents comply with the requirements of these Regulations and internal rules.

7.26. The Bank shall be liable for violation by its payment agents and payment subagents of the requirements of these Regulations.

7.27. The following information must be recorded and stored electronically:

a) a list of persons provided by the Department;
b) identified suspicious transactions;
c) suspicious transactions reported to the Department;
d) customers included in the high-risk category;
e) international payments, including operations on international money transfers;
f) operations with international plastic cards.

VIII. QUALIFICATION REQUIREMENTS FOR THE TRAINING AND INSTRUCTION OF THE INTERNAL CONTROL STAFF

8.1. Commercial banks shall conduct regular retraining of employees of the Internal Control Service, bank departments directly serving customers (responsible executives, cashiers, etc.), legal services, internal audit and security services, in order to ensure that employees are aware of the latest innovations, including information on modern technique of money laundering and terrorist financing, methods and trends, and a clear explanation of all aspects of legislation and obligations to combat money laundering and financing of terrorism.

8.2. The Internal Control Service shall, together with the relevant divisions of the Bank, annually develop a training, retraining and training program for employees of a commercial bank on combating money laundering and financing of terrorism (hereinafter referred to as the training program). This program should include the following:

- procedure for conducting training, its forms (primary briefing, scheduled and unscheduled training) and terms;
- appointment of persons responsible for organizing the training;
- procedure for checking knowledge.

The training program shall be approved by the Management Board of the Bank.

8.3. Before taking up their official duties, employees hired by departments that directly carry out banking operations (departments of retail operations, plastic cards, money circulation, corporate services for legal entities, lending, foreign exchange operations, back office, cash desk, mini-banks, etc. .) shall have an initial briefing by an employee of the internal control service on the issues of combating money laundering and financing of terrorism.

Human Resources Department Manager or the employee performing its duties shall send employees hired to the departments that directly carry out banking operations to the employee of the Internal Control Service to receive an initial briefing.

8.4. The initial briefing shall include the following issues:

- customer due diligence rules;
- essence of assigning a customer risk category, criteria for customers and operations related to a high risk level;
- criteria and signs of doubtful and suspicious transactions, actions of the employee when such transactions are identified;
- requirements to ensure the confidentiality of information on combating money laundering and financing of terrorism;
- other issues.

An employee, who has passed the initial briefing, shall sign an obligation in the form of Annex No. 15, on familiarization and compliance with the Regulations for combating money laundering and financing of terrorism.

8.5. The Internal Control Service, together with the Human Resources Department and other departments, shall develop a training plan for seminars that include issues of combating money laundering and financing of terrorism, as well as preventing offenses committed by bank employees.

Planned training must be carried out in each branch at least once a quarter. The topics of planned training should be varied and, in addition to internal control regulations, cover

issues of international requirements and organizations for combating money laundering and financing of terrorism, shortcomings and omissions made in the Bank's divisions (departments of lending, money circulation, corporate services for legal entities , foreign exchange transactions, etc.), technical areas, carried out in order to improve the quality of customer service and strengthen internal control.

8.6. In the event of a change in the legislation on combating money laundering and financing of terrorism or introduction of innovations in this area, when developing or implementing new business practices in order to improve the efficiency of the Bank's Internal Control Service, or at the direction of the Chairman of the Management Board, unscheduled training sessions may be arranged.

8.7. In order to increase the effectiveness and attractiveness of training sessions on the topic of combating money laundering and financing of terrorism, it is necessary to use interactive teaching methods, in particular slides, handouts, etc.

8.8. The Bank shall conduct regular retraining of employees in order to ensure that employees are aware of the latest developments, including information on modern technology of money laundering and terrorist financing, methods and trends, and a clear explanation of all aspects of legislation and obligations to combat money laundering and financing of terrorism.

8.9. In order to test the knowledge on combating money laundering and financing of terrorism of employees carrying out operations of the Bank, it is necessary to conduct their certification in accordance with the terms and procedure established by the program approved by the Management Board of the Bank.

8.10. The following requirements must be reflected in the Job Descriptions of all employees engaged in banking operations:

- facts and procedure for customer due diligence, knowledge of the criteria for doubtful and suspicious transactions, as well as customers belonging to the high-risk category;
- immediate submission of a notice to the Internal Control Service and immediate supervisor in case of revealing doubtful and suspicious transactions;
- when contacting an employee directly serving the customer to provide additional information on behalf of the Internal Control Service, contact the customer in accordance with the established procedure and bring the information received to the Internal Control Service;
- promptly and correctly, identify the customer and fill out the electronic questionnaire (for employees who are entrusted with these duties).

8.11. Manager of the Internal Control Service, in order to improve his own knowledge and qualifications, as well as the knowledge and qualifications of employees and familiarize himself with the latest innovations, shall organize technical training. In addition, assessing the knowledge of employees, if necessary, take measures to send employees who need to improve their knowledge to training courses.

Manager of the Internal Control Service shall have up-to-date knowledge and the latest innovations and requirements in the field of combating money laundering and financing of terrorism. To this end, the Manager of the Internal Control Service, together with the Human Resources Department, shall take measures to find and participate in international courses and seminars, and shall make a proposal to the Chairman of the Management Board on participation in them.

IX. RELATIONSHIP OF THE INTERNAL CONTROL SERVICE WITH OTHER DIVISIONS OF THE BANK

9.1. In carrying out its activities, the Internal Control Service shall enter into relationships with other divisions.

9.2. The Internal Control Service shall interact with Accounting and Reporting Department,

Money Circulation and Retail Operations Department, as well as in branches with the departments of Corporate Services for Legal Entities, Retail Operations and Plastic Card Services, and Cash Operations on the following issues:

- relevant employees of these departments identify customers and their real owners, enter the information obtained using programs into the customer's questionnaire (card);
- at the request of the Internal Control Service, submit documents (legal folders) obtained as a result of customer due diligence;
- relevant employees of these units can contact the internal control service to clarify the information received on public officials identified during the customer due diligence.

9.3. The Internal Control Service shall enter into relationships with departments for foreign economic activity, lending, money circulation, plastic card servicing on the following issues:

- employees of these divisions, at the request of the Internal Control Service, shall analyze suspicious transactions or verify customer transactions, submit relevant documents (export-import contracts, documentary transactions, folders for conversions, credit folders, documents collected from transfers of household income to deposit accounts);
- provide reports required by the Internal Control Service.

9.4. It shall enter into relations with the Information Technology Department on the following issues:

- The Information Technology Department, in order to perform its functions by the Internal Control Service, shall provide computer technology, communications, programs and other technical means, take measures to create the possibility of using all types of data available in the bank's automated system;
- The Information Technology Department, at the request of the Internal Control Service, shall create and improve the software necessary for its activities (database on customers that help identify dubious and suspicious transactions, etc.);

9.5. All divisions of the Bank working with customers shall interact with the Internal Control Service on the following issues:

- if dubious transactions are revealed during the current audit of the customer’s operations, they shall immediately inform their immediate supervisor and employees of the Internal Control Service about such transactions in writing;
- if suspicious transactions are identified on behalf of the Internal Control Service, if necessary, they shall apply to the customer for additional information about the operation being carried out;

9.6. The departments of the Bank that control and coordinate activities of all departments involved in the internal control system, especially Accounting and Reporting Department, Monetary Circulation and Retail Operations Department, Foreign Economic Affairs Department and other departments should also control the compliance with the requirements of the anti-money laundering and financing of terrorism legislation by the respective supervised departments in the branches. In addition, when the Internal Control Service appeals to the departments to eliminate the shortcomings allowed by the relevant departments under their control, ways to strengthen control by the relevant departments, they should show solidarity and respond appropriately.

9.7. In addition, the Internal Control Service shall cooperate with:

- the Banking Risk Management Department in preventing errors and violations that may arise as a result of operational and credit risk, developing draft internal acts and determining the job responsibilities of bank employees;
- the Banking Security Department on the issue of conducting inspections in order to analyze the customer's operations;
- the Legal Department, in order to study typical cases of violations of regulations and legislation of the Republic;
- the Human Resources Department on employee training, improving their professional skills, as well as on conducting technical training and tests.

9.8. The Internal Audit Department shall inform the Internal Control Service of the shortcomings identified in the course of inspections of the activities of the Bank's divisions, in particular, about the facts of operations for money laundering and cases of its concealment in order to respond appropriately on it. It also shall make its proposals for further improvement of the internal control system in the Bank.

The Internal Control Service has the right to consult with the Internal Audit Department on issues arising in the course of activities, as well as on other issues.

X. EXERCISING CONTROL OVER THE IMPLEMENTATION OF THE INTERNAL CONTROL REGULATIONS

10.1. Monitoring and control over compliance by commercial banks with the requirements of these Regulations shall be carried out by the Internal Control Service.

10.2. Based on the plan made by the employees of the Internal Control Service, the branches shall conduct checks on the effectiveness of the internal control system and compliance with the requirements of these Regulations at least once a year. In newly opened branches, for the purpose of the initial correct organization of the internal control system, an audit shall be carried out no later than three months from the date of opening the branch.

If the Manager of the Internal Control Service is sent for inspection, its duties shall be performed by another employee of the Internal Control Service.

10.3. In order to control the fulfillment by the Bank and its branches of the requirements of the internal control Regulations on combating money laundering and financing of terrorism, employees of the Internal Control Service shall conduct intermediate monitoring at the end of each month until the 10th day of the next month. In carrying out intermediate monitoring, they should pay attention to the following issues:

- correct customer due diligence, including one-off transactions;
- taking appropriate measures to identify public officials in the process of customer due diligence;
- timely and correct completion of electronic customer questionnaires;
- timely introduction of appropriate changes in the electronic customer questionnaires, in cases of changes in the identification data of the customer;
- timely full notification of transactions that meet the criteria for doubtful and suspicious transactions under export-import contracts and international payments;
- full notification of dubious and suspicious transactions on money transfers of individuals;
- full notification of doubtful and suspicious operations with plastic cards;
- full and timely notification of transactions carried out in the national currency that have the criteria and signs of doubtfulness or suspicion provided for in clauses 4.1.1-4.1.2 of these Regulations;
- other issues.

When employees of the internal control service request information and documents requested as part of issues including intermediate monitoring, including legal folders, identification information, electronic forms of certain transactions and others, they must be provided in a timely manner by the relevant departments and departments.

10.4. In case of revealing doubtful and suspicious transactions during the interim monitoring by employees of the Internal Control Service, it is necessary to pay attention to the provision of reports about them by the relevant employees in the prescribed manner.

Doubtful and suspicious transactions, for which no reports were submitted, shall be studied and an appropriate decision shall be made on it. After that, the reason for the timely failure to provide information about these operations to employees of the internal control service shall be established.

10.5. The relevant employees of the Bank shall be responsible for failure to provide information

about suspicious transactions and for its concealment.

10.6. Based on the results of interim monitoring, a certificate shall be issued, and its copies shall be submitted to the Manager of the internal control service and the Branch Manager no later than the 12th day of the month in the prescribed manner.

The Branch Manager shall study the identified shortcomings and report it to Managers of the relevant departments, and measures shall be taken to eliminate them and prevent them in the future.

Manager of the internal control service shall study the results of the monthly monitoring conducted in all branches by employees of the internal control service, draw up a summary statement and submit it to the Chairman of the Management Board no later than the 15th day of the month. If gross errors and deficiencies are identified, if errors are systematically made, as well as in case of untimely elimination of identified errors and deficiencies, the Manager of the internal control service can give recommendations to the Chairman of the Management Board on improving the internal control system, taking measures against guilty employees.

10.7. The Bank's Management Board, taking into account changes in external and internal situations shall constantly monitor the Bank's internal control system and take measures to strengthen its activities to ensure efficient operation.

10.8. The effectiveness of the internal control system may be monitored by the Internal Audit Service of the Bank. In order to monitor the effectiveness of the internal control system in the field of combating money laundering, financing of terrorism and financing of the proliferation of weapons of mass destruction, as well as confirming the compliance of the Bank's internal procedures, an Independent External Audit may also be carried out. The frequency of such verification shall be determined by the Bank independently, while the frequency cannot be less than once in 2 years.

10.9. Shortcomings in the internal control system identified by the Internal Audit Service, Independent External Audit or other control services shall be timely brought to the attention of the Chairman of the Management Board of the Bank. After receiving such information, the Chairman of the Management Board shall take measures to eliminate the identified shortcomings in a timely manner.

10.10. In order to strengthen and improve the efficiency of internal control to combat money laundering and financing of terrorism, to discuss the results of an audit conducted by the Internal Audit Service in relation to compliance with the requirements of the legislation on internal control, the Management Board of the Bank shall hold a meeting at least once a year, if necessary, with the invitation of Managers of the relevant departments or branches.

Annex No. 1
to the Regulations of internal control on combating money laundering and financing of terrorism at "Asia Alliance Bank" JSCB

INFORMATION
required for identification of individuals

1. Surname, name and patronymic.
2. Date and place of birth.
3. Citizenship.
4. Place of permanent and (or) temporary residence.
5. Details of the passport or a document replacing it: the series and number of the document, the date of issue of the document, name of the authority that issued the document.
6. Personal identification number of an individual. (PINFL)
7. Tax identification number (if any).
8. Residence and mobile phone number (if available).
9. Email address (if available).

Annex No. 2
to the Regulations of internal control on combating money laundering and financing of terrorism at "Asia Alliance Bank" JSCB

INFORMATION,
required for the identification of legal entities and individual entrepreneurs

1. Information required for the identification of legal entities:

   a) full name, as well as the abbreviated name, if it is indicated in the certificate of state registration;
   b) information on state registration: date, number, name of the registering authority;
   c) date of initial registration of the enterprise (or its successor)
   d) taxpayer identification number;
   e) location (postal address);
   f) other data specified in the certificate of state registration;
   g) information on available licenses to carry out types of activities subject to licensing: type of activity, number and date of issue of the license; issued by whom; validity;
   h) data on the identification of individuals who have the right to sign, or an individual acting on behalf of a legal entity;
   i) information about the founders (major shareholders, participants) and their equity participation in the authorized capital (fund) of the legal entity;
   j) information on the amount of the registered and paid authorized fund (capital);
   k) information about the management bodies of the legal entity (the structure and personnel of the management bodies of the legal entity);
   l) phone numbers;
   m) Web site and e-mail address (if available).

2. Information required for the identification of individual entrepreneurs:

   a) information provided for in Annex No. 1 to these Regulations;
   b) information on state registration: date, number, name of the registering authority;
   c) place of business;
   d) other data specified in the certificate of state registration;
   e) information on available certificates and licenses for activities: type of activity, number, date of issue; issued by whom; validity;
   f) telephone numbers;
   g) Web site and e-mail address (if any).

Annex No. 3
to the Regulations of internal control on combating money laundering and financing of terrorism at "Asia Alliance Bank" JSCB

INFORMATION,
specified in the customer's questionnaire

1. Information received in the process of customer identifying, specified in Annexes No. 1 and 2 to these Regulations.
2. Information about the level of risk, including the rationale for the risk assessment.
3. The results of additional activities carried out by the bank when customer identifying.
4. Date of commencement of relations with the customer - the date of opening the first bank account (deposit) in a commercial bank.
5. Date of filling in and making changes to the customer's questionnaire.
6. Surname, name and patronymic, title of the employee responsible for working with the customer, in particular, the employee who opened the account (Chief Accountant or his deputy) and approved the opening of the account.
7. Signature of the employee who filled out the customer's questionnaire on paper (indicating the last name, first name and patronymic, position) and the last name, first name and patronymic, title of the employee who filled out the customer's questionnaire in electronic form.
8. Other data determined by internal Regulations.

Annex No. 4
to the Regulations of internal control on combating money laundering and financing of terrorism at "Asia Alliance Bank" JSCB

ASIA ALLIANCE BANK

CORRESPONDENT BANK QUESTIONNAIRE
(for CIS countries)

I. General Data */

1.1. Name of the Bank (according to the Articles of Association)			
a) Full and abbreviated name in Russian:: b) Abbreviated name in a foreign language:			
1.2. Organizational and legal form			
1.3. Information about state registration			
a) State Registration Authority: b) Date of state registration: c) State registration number: d) Place of state registration: e) Document certifying state registration:			
1.4. Taxpayer identification number (TIN)		**1.6. Codes of state statistical observation forms**	
		OKPO	
1.5. Bank Codes		OKOGU	
Bank Identification Code (BIC)		OKATO	
SWIFT		OKVED	
TELEX		OKFC	
		OKOPF	
1.7. Licenses (permits) for certain banking operations			
a) Type of license: b) Issuing authority: c) License issue date: d) License number:			
1.8. Address			
a) Legal address: b) Postal address			
1.9. Contacts			
a) Phones: b) Fax:		c) Official WEBSITE: d) Email address:	

*/ All lines of the questionnaire must be filled in, in the absence of information on any line, you should note: "data is not available."

II. Data on the structure and position in the market

2.1. Information about the main founders/participants (whose share is 10% or more): name, location address **/
2.2. Information about governing bodies (structure and personnel staff)

2.3. A person who has the right to act on behalf of the Bank without a power of attorney
2.4 Information about the Authorized Fund
a) Registered: b) Paid:
2.5. Information about subsidiaries and affiliates
2.6. Information about the main correspondent banks
2.7. History, reputation, market sector and competition (e.g. link to Bankers Almanac)
2.8. Information about the name of the external audit organization that audits the reliability of the bank's financial statements, with the last audit date
2.9. Availability of a rating assigned to the Bank by an international rating agency (Moody`s Investors Service, Standard & Poor`s or Fitch Ratings)
2.10. Does the financial institution carry out the following financial transactions:
- Placement of attracted funds on its own behalf, on its own terms and at its own risk; ☐ *Yes* ☐ *No*
- Opening correspondent accounts in authorized banks of your country in a foreign currency and transactions on it; ☐ *Yes* ☐ *No*
- Operations with banking metals in the foreign exchange market of your country; ☐ *Yes* ☐ *No*
- Organization of purchase and sale of securities under the guarantees of customers; ☐ *Yes* ☐ *No*
- Acquisition of the right to claim the fulfillment of obligations in cash for the goods supplied or services provided, assuming the risk of fulfilling such claims and accepting payments (factoring); ☐ *Yes* ☐ *No*

****/** Specify whether there are public officials among the founders and shareholders

III. Measures aimed at combating money laundering and financing of terrorism

3.1. List the laws and regulations aimed at preventing money laundering and the involvement of banks in illegal transactions operating in your country. Is your Bank the unconditional executor of these laws?
3.2. What regulatory documents regulate the procedures for exercising compliance control in your Bank aimed at preventing money laundering and financing of terrorism (AML/CFT)? */**
3.3. Availability and name of a structural unit performing functions related to AML/CFT
3.4. Information about the responsible employee of the compliance control service
a) Full name: b) Title: c) Contact phone: d) e-mail:
3.5. Does your bank have controls in place to combat terrorist financing? If so, which ones?
☐ *Yes* ☐ *No*

3.6. Does your bank apply the Know Your Customer (Customer Identification) principle? Please provide detailed information.
☐ *Yes* ☐ *No*
3.7. Does your bank's branches (if any) have internal control procedures in place to counter money laundering?
☐ *Yes* ☐ *No*
3.8. Are anti-money laundering procedures in place in your foreign branches and subsidiaries?
☐ *Yes* ☐ *No*
3.9. Does your Bank have an AML training program for employees? Please provide detailed information.
☐ *Yes* ☐ *No*
3.10. Does your institution have an account and transaction tracking system in place to detect suspicious activity? Is there software, if so, please provide information.
☐ *Yes* ☐ *No*
3.11. How do you determine the source of origin of funds credited to your customer's account?
3.12. What criteria are used in your Bank to assess the level of risk of the customer's legalization of illegally obtained income?
3.13. Information on the availability of branches and representative offices in states (territories) that do not participate in international cooperation in the field of AML/CFT
3.14. Does your Bank maintain correspondent relationships with banks registered in states and territories with a preferential tax regime (or) that do not provide for the disclosure and provision of information when conducting financial transactions (the so-called offshore zones)? If yes, please list those correspondent banks.
☐ *Yes* ☐ *No*
3.15. Does your Bank establish correspondent relationships with banks that do not have a physical presence in any country (the so-called "Shell Banks")?
☐ *Yes* ☐ *No*
3.16. Does your institution have a procedure to prevent the opening of accounts for individuals and legal entities involved in the legalization (laundering) of incomes and terrorist activities that are on the OFAC/EU/UN "black list"? **Provide detailed information.**
3.17. Have your Bank been investigated for violations related to money laundering and financing of terrorism?
☐ *Yes* ☐ *No*
3.18. Is your Bank able to provide identification data about the customer at the request of our Bank in order to study the operation?
☐ *Yes* ☐ *No*

***/ Specify the name of the document, number and date of its adoption

Confirmation: (the signatory certifies that the above questionnaire contains a true information.

Head of the Bank:

(Title) _____ (signature) (Full Name)

Compliance Control Employee:

(Title) _____ (signature) (Full Name)

Seal **Date: « » 20**

Annex No. 5
to the Regulations of internal control on combating money laundering and financing of terrorism at "Asia Alliance Bank" JSCB

ASIA ALLIANCE BANK

Questionnaire

(to be filled by a partner financial institution)

I. General Information

1.1. Full legal name of financial institution (FI)			
1.2. Legal Form (for example Public Limited Company, Joint Stock Company, Partnership, but this is not exhaustive etc.)			
1.3. Legal address			
1.4. Mailing address			
1.5. Registration/License No		**1.6. Date of registration**	
1.7. Registration body			
1.8. Type of license			
1.9. License number		**1.10. Date of issue of the license**	
1.11. SWIFT, TELEX			
1.12. FI contacts		**1.13. Key contact person**	
Telephone		Name:	
Fax		Title	
Website address		Telephone	
e-mail		e-mail	

II. Ownership, management and regulatory information

2.1. If FI is publicly held, please indicate exchange on which shares are traded:		
2.2. If Institution is privately owned, please list the names of all owners in the table below and their ownership interest (add further rows if necessary)		
Name	Domicile (country, city)	Ownership

		interest (%)

2.3. Supervisory Council

Name	Domicile (country, city)	Main type of activity

2.4. Executive Management / Board of Directors of Institution

Name	Domicile (country, city)	Position

2.5. Have there been any significant changes in ownership (exceeding 25%) over the last five years?

☐*Yes* ☐*No*

If yes, please provide details:

2.6. Please indicate the ultimate beneficial owner(s) of your FI, if any, including personal data (i.e. place and date of birth, domicile).

For the meaning of "Beneficial Owner" please refer to the definition given at the end of this questionnaire.

2.7. Does your Bank have branches, subsidiaries, affiliates and representative offices?

☐*Yes* ☐*No*

If yes, specify them

2.8. Name of your Financial Intelligence Unit (FIU)

2.9. Are your FI subject to external audit activities?

☐*Yes* ☐*No*

If yes, please provide the name of your external auditors. (An external auditor does not mean the Central Bank or Government Body)

III. Anti-Money Laundering and Counter Terrorist Financing

(If you answer "no" to any question, additional information can be supplied at the end of the questionnaire)

A. General AML Policies, Practices and Procedures:	**Yes**	**No**
3.1. Is the AML compliance program approved by the FI's board or a senior committee?	☐	☐
3.2. Does the FI have a legal and regulatory compliance program that includes a designated officer that is responsible for coordinating and overseeing the AML framework?	☐	☐
3.3. Has the FI developed written policies documenting the processes that they have in place to prevent, detect and report suspicious transactions?	☐	☐
3.4. In addition to inspections by the government supervisors/regulators, does the FI client have an internal audit function or other independent	☐	☐

third party that assesses AML policies and practices on a regular basis?		
3.5. Does the FI have a policy prohibiting accounts/relationships with shell banks?	☐	☐
3.6. Does the FI have policies to reasonably ensure that they will not conduct transactions with or on behalf of shell banks through any of its accounts or products?	☐	☐
3.7. Does the FI have policies covering relationships with Politically Exposed Persons (PEP's), their family and close associates?	☐	☐
3.8. Does the FI have record retention procedures that comply with applicable law?	☐	☐
3.9. Are the FI's AML policies and practices being applied to all branches and subsidiaries of the FI both in the home country and in locations outside of that jurisdiction?	☐	☐
3.10. Has your FI had any regulatory or criminal enforcement actions resulting due to violations of anti-money laundering laws or regulations?	☐	☐
B. Risk Assessment	**Yes**	**No**
3.11. Does the FI have a risk-based assessment of its customer base and their transactions?	☐	☐
3.12. Does the FI determine the appropriate level of enhanced due diligence necessary for those categories of customers and transactions that the FI has reason to believe pose a heightened risk of illicit activities at or through the FI?	☐	☐
C. Know Your Customer, Due Diligence and Enhanced Due Diligence	**Yes**	**No**
3.13. Has the FI implemented processes for the identification of those customers on whose behalf it maintains or operates accounts or conducts transactions?	☐	☐
3.14. Does the FI have a requirement to collect information regarding its customers' business activities?	☐	☐
3.15. Does the FI assess its FI customers' AML policies or practices?	☐	☐
3.16. Does the FI have a process to review and, where appropriate, update customer information relating to high risk client information?	☐	☐
3.17. Does the FI have procedures to establish a record for each new customer noting their respective identification documents and 'Know Your Customer' information?	☐	☐
3.18. Does the FI complete a risk-based assessment to understand the normal and expected transactions of its customers?	☐	☐
3.19. Does your FI ability to provide essential identification data about the client according to the inquiry of the bank respondent in order to examine operations?	☐	☐
D. Reportable Transactions and Prevention and Detection of Transactions with Illegally Obtained Funds	**Yes**	**No**
3.20. Does the FI have policies or practices for the identification and reporting of transactions that are required to be reported to the authorities?	☐	☐
3.21. Where cash transaction reporting is mandatory, does the FI have procedures to identify transactions structured to avoid such obligations?	☐	☐
3.22. Does the FI screen customers and transactions against lists of persons, entities or countries issued by government/competent authorities?	☐	☐
3.23. Does the FI have policies to reasonably ensure that it only operates with correspondent banks that possess licenses to operate in their countries of origin?	☐	☐
E. Transaction Monitoring	**Yes**	**No**
3.24. Does the FI have a monitoring program for unusual and potentially suspicious activity that covers funds transfers and monetary instruments such as travelers checks, money orders, etc?	☐	☐
F. AML Training	**Yes**	**No**
3.25. Does the FI provide AML training to relevant employees that includes:	☐	☐

▪ Identification and reporting of transactions that must be reported to government authorities. ▪ Examples of different forms of money laundering involving the FI's products and services. ▪ Internal policies to prevent money laundering.		
3.26. Does the FI retain records of its training sessions including attendance records and relevant training materials used?	☐	☐
3.27. Does the FI communicate new AML related laws or changes to existing AML related policies or practices to relevant employees?	☐	☐
3.28. Does the FI employ third parties to carry out some of the functions of the FI?	☐	☐
3.29. If the answer to question 26 is yes, does the FI provide AML training to relevant third parties that includes: ▪ Identification and reporting of transactions that must be reported to government authorities. ▪ Examples of different forms of money laundering involving the FI's products and services. ▪ Internal policies to prevent money laundering.	☐	☐

Space for additional information:
(Please indicate which question the information is referring to.)
.....
.....
.....
.....
.....
.....

I confirm that, to the best of my knowledge, the above information is current, accurate and reflective of my institution's anti-money laundering policies.	
Signature:	
Title:	
Date:	

(Seal)

In this questionnaire the following references are used:

- "Beneficial owner" means the natural person(s) who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted. The beneficial owner shall at least include:
  a) in the case of corporate entities:
     (i) the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity, including through bearer share holdings, other than a company listed on a regulated market that is subject to disclosure requirements consistent with Community legislation or subject to equivalent international standards; a percentage of 25 % plus one share shall be deemed sufficient to meet this criterion;
     (ii) the natural person(s) who otherwise exercises control over the management of a legal entity:
  b) in the case of legal entities, such as foundations, and legal arrangements, such as trusts, which administer and distribute funds:
     (i) where the future beneficiaries have already been determined, the natural person(s) who is the beneficiary of 25 % or more of the property of a legal arrangement or entity;
     (ii) where the individuals that benefit from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;

(iii) the natural person(s) who exercises control over 25 % or more of the property of a legal arrangement or entity.

- “Politically exposed person” means natural persons who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons.
- “Shell banks” means a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group.

Annex No. 6
to the Regulations of internal control on combating money laundering and financing of terrorism at "Asia Alliance Bank" JSCB

Requirements for Entering Data into Electronic Customer Questionnaires

1. Customer questionnaires shall be filled in by the relevant employees before the transaction, no later than the date of the first account opening.
2. All boxes (fields) of the questionnaire, subject to mandatory completion, must be filled in completely, and optional boxes must be filled in completely as far as possible. Data intended to be entered in a particular box cannot be written in other boxes.
3. All information shall be recorded in Uzbek, which is the state language, unless otherwise specified in the identity document (for individuals) or the document confirming state registration (for legal entities).
4. The names of customers must be entered in exact accordance with the entries in the identity document (individuals) or the document confirming state registration (legal entities).
5. The surname, name, patronymic of individuals shall be entered in the identity document recorded in the identity document (Cyrillic, Latin, etc.) and only in capital letters, unless otherwise specified in this document.
6. When entering the name of legal entities, the name is first recorded, and then the organizational and legal form and form of ownership, unless otherwise stated in the state registration document. Names of resident legal entities shall be written in quotation marks. When recording the abbreviated name of legal entities, the following abbreviations shall be used: private enterprise - PE, limited liability company - LLC, joint venture - JV, foreign enterprise - FE.

   The names of legal entities in Russian and foreign languages shall be recorded in exact accordance with the entries in their constituent documents.
7. When a legal entity submits several documents on state registration or constituent documents, the information of the latter shall be entered, that is valid.
8. The name of the customer, addresses, and other data of the questionnaire must be entered without errors, and additional characters (spaces, quotation marks, dashes) are not used.
9. Information about whether the customer is a resident or non-resident must be specified accurately.
10. Address of the customer shall be recorded in descending order as follows: postal code, region, city or district, rural community of citizens, mahalla, street, house, and apartment. Each name shall be separated by a comma. The following abbreviations shall be used: region - vil., city - sh., district - tum., rural community of citizens - Ҷ.F.Y., street - kuch. Addresses of foreign customers shall be recorded in accordance with the specified data in the document.
11. The name of the body that issued the identity document of individuals, as well as the name of the body that carried out state registration of legal entities, shall be recorded in the order specified in the document, without separation by commas, while abbreviation is not used. For example: Toshkent shahar Shayhontohur tumani IIB, Toshkent viloyati Qibray tumani hokimiyati, etc. Foreign authorities shall be recorded in accordance with the specified data in the document.
12. When making changes to the available customer identification data, employees of the relevant departments shall make appropriate changes to the customer's questionnaire and inform the employees of the Internal Control Service about this.

Annex No. 7
to the Regulations of internal control on
combating money laundering and financing
of terrorism at "Asia Alliance Bank" JSCB

Internal Control Service

Notification

In accordance with Clause 64 of the Internal Control Regulations on Combating Money Laundering and Financing of Terrorism in Commercial Banks, registered on May 23, 2017 with the Ministry of Justice under No. 2886, I am notifying about doubtful/suspicious (delete as applicable) operation identified during the current audit of the customer's operation:

Date of operation: _____
Type of document (operation): _____
Name of the payer: _____
(if non-resident, the state shall be specified)
Payer's bank name: _____ Bank code: _____
Beneficiary name: _____
(if non-resident, the state shall be specify)
Name of beneficiary's bank: _____ Bank code: _____
Transaction amount _____
(amount in figures and words, name of currency)
_____
Subject of payment: _____
_____
Criteria or sign of doubtful/suspicious operation: _____
_____

Employee who submitted the report:
Title _____ _____ Full name _____
(signature)

Date _____

A notification received by:
Title _____ _____ Full name _____
(signature)
Date _____

Criteria assigned by an employee of the internal control:

Transaction type	Number of criteria

Annex No. 8
to the Regulations of internal control on
combating money laundering and financing
of terrorism at "Asia Alliance Bank" JSCB

Register of notifications on suspicious transactions submitted by employees

(left part)

№	Transaction date	Customer's name	Customer's unique ID	Name and country of the correspondent	Correspondent Bank (by MFO or SWIFT)	Payment type (incoming, outgoing)	Transaction amount and currency

(right part)

Transaction subject	Notification date	Full Name of the reporting employee	Transaction criteria		Measures taken on transaction	Notification date to the Head Office
			Doubtful	Suspicious		

Annex No. 9
to the Regulations of internal control on
combating money laundering and
financing of terrorism at "Asia Alliance
Bank" JSCB

Register of reports on suspicious transactions submitted to the Department

(left part)

№	Transaction date	Customer's name	Customer's unique ID	Name and country of the correspondent	Correspondent Bank (by MFO or SWIFT)	Payment type (incoming, outgoing)	Transaction amount and currency

(right part)

Transaction subject	Notification date	Full Name of the reporting employee	Transaction criteria		Measures taken on transaction	Notification date to the Department
			Doubtful	Suspicious		

Annex No. 10
to the Regulations of internal control on
combating money laundering and financing
of terrorism at "Asia Alliance Bank" JSCB

Register of customer's instructions (documents) whose operations are terminated

№	Transaction date	Document number and date	Customer's Name	Name and country of the correspondent	Correspondent bank (by MFO or SWIFT) or money transfer system	Transaction amount and currency	Subject of transaction	Date of transactions termination	Notes

Annex No. 11
to the Regulations of internal control on combating
money laundering and financing of terrorism at
"Asia Alliance Bank" JSCB

Schedule for recording cash withdrawals from plastic cards of other banks through the terminal ASIA ALLIANCE BANK

№	Transaction date	Customer's name	Passport series	Passport number	Plastic card number	Code of the bank that issued the plastic card	Name of the bank that issued the plastic card	Transaction amount

Annex No. 12
to the Regulations of internal control on combating
money laundering and financing of terrorism at
"Asia Alliance Bank" JSCB

Schedule for recording of payments for goods and services from plastic cards of other banks through the terminal "ASIA ALLIANCE BANK"

№	Transaction date	Customer's name	Passport series	Passport number	Plastic card number	Code of the bank that issued the plastic card	Name of the bank that issued the plastic card	Name of the beneficiary	Account of the beneficiary	Code of the beneficiary's bank	Name of the beneficiary's bank	Details of payment	Transaction amount

Annex No. 13
to the Regulations of internal control on combating money laundering and financing of terrorism at "Asia Alliance Bank" JSCB

Schedule for recording of non-cash payments for goods and services by individuals without opening a personal account (through transit accounts)

№	Transaction date	Customer's name	Passport series	Passport number	Transit account number	Name of the transit account	Name of beneficiary	Beneficiary's account	Code of beneficiary's bank	Name of beneficiary's bank	Details of payment	Transaction amount

Annex No. 14
to the Regulations of internal control on combating money laundering and financing of terrorism at "Asia Alliance Bank" JSCB

Schedule for recording of detected suspicious and suspicious transactions

№	Date of the first operation	Last date of the operation	Customer's name	Customer's code	Correspondent name	Correspondent country name	Correspondent bank or money transfer system	Correspondent bank code	Payment method (incoming, outgoing)	Transaction amount	Currency code	Payment purpose

Criteria		Full name of the employee who sent the message	Date of notification to ICS or date of detection by the ICS employee	Date of notification to the ICS of the Head Office	File of the message from the Branch	Code of the branch	Date of notification to the Department	Name of the notification file to the Department	Reference of the message to the Department
Doubtful	Suspicious								

Annex No. 15
to the Regulations of internal control on
combating money laundering and financing
of terrorism at "Asia Alliance Bank" JSCB

COMMITMENT
on compliance with the Regulations for combating money laundering and financing of terrorism

I am, _____
(Department, Title, Full Name)

Familiarized with the Regulations of internal control on combating money laundering and financing of terrorism at JSCB "Asia Alliance Bank".

Gained sufficient knowledge of questionable and suspicious transactions, as well as customers and transactions classified as high-risk, as defined by the Regulations.

I undertake to continue to perform the following functions provided for in these Regulations:

☐ perform customer due diligence in the prescribed manner;

☐ in case of revealing doubtful and suspicious transactions, immediately inform the Internal Control Department and the immediate supervisor about this in writing;

☐ when contacting an employee directly serving the customer to provide additional information as instructed by an employee of the Internal Control Department, contact the customer in accordance with the established procedure and bring the information received to the Internal Control Department.

☐ be aware of states not participating in international cooperation in the field of combating money laundering and financing of terrorism and offshore zones;

☐ improve knowledge and skills in the field of combating money laundering and financing of terrorism. Participate in trainings organized by the Bank on this topic.

_____	_____	_____
(Full Name)	(signature)	(date)