POLICY OF JSC «REALIST BANK»
in order to counter the legalization (laundering) of proceeds from crime, the financing of terrorism and the financing of the proliferation of weapons of mass destruction

(AML/CFT/FPWMD POLICY)

MOSCOW
Update as at 2023.05.25

TABLE OF CONTENTS

1. GENERAL PROVISIONS

The internal control policy in order to counter the legalization (laundering) of proceeds from crime, the financing of terrorism and the financing of the proliferation of weapons of mass destruction REALIST BANK JSC (hereinafter referred to as the Rules) was developed in pursuance of the legislation of the Russian Federation in the field of countering the legalization (laundering) of proceeds from crime criminal means, financing of terrorism and financing of the proliferation of weapons of mass destruction (hereinafter referred to as AML/CFT/FPWMD), regulations of the Bank of Russia and the Federal Financial Monitoring Service.

The policy complies with internal regulations and includes internal control programs.

The main principles and goals of organizing internal control in the Bank in order to counteract the legalization (laundering) of proceeds from crime, the financing of terrorism and the financing of the proliferation of weapons of mass destruction are:

- ensuring the protection of the Bank from the penetration of criminal proceeds into it;
- managing the risk of legalization (laundering) of proceeds from crime and financing of terrorism in order to minimize it;
- ensuring the independence of the Bank's Responsible Officer; participation of employees of the Financial Monitoring Department responsible for the organization of the AML/CFT/FPWMD system and the implementation of the AML/CFT/FPWMD Internal Control Rules, the Bank’s divisions involved in banking operations and other transactions, the Legal Department, the Economic Security Department, the Internal Control Service, the Internal Control Service audit of the Bank, regardless of their position, within their competence in identifying transactions subject to mandatory control, and transactions in respect of which there are suspicions that they are carried out for the purpose of legalization (laundering) of proceeds from crime, financing of terrorism and financing the proliferation of weapons of mass destruction , as well as in identifying a set of transactions and (or) actions of the client,

Objectives of this policy:

- ensuring that the Bank complies with the requirements of the legislation in the field of AML/CFT/FPWMD ;
- maintaining the effectiveness of the Bank's AML/CFT/FPWMD internal control system at a level sufficient to manage the risk of legalization (laundering) of proceeds from crime, financing of terrorism and financing the proliferation of weapons of mass destruction;
- excluding the involvement of the Bank, its managers and employees in the legalization (laundering) of proceeds from crime, the financing of terrorism and the financing of the proliferation of weapons of mass destruction.

The AML/CFT/FPWMD policy is kept up to date, in accordance with the requirements of the Russian Federation legislation in the field of AML/CFT/FPWMD .

2. PROGRAM FOR THE ORGANIZATION OF THE AML/CFT/FPWMD SYSTEM

Internal control for AML/CFT/FPWMD purposes is part of the Bank's internal control system and is carried out by the Bank's divisions and employees on an ongoing basis.

Internal controls for AML/CFT/FPWMD purposesfunctions in the Bank at the following levels:

- Board of Directors of the Bank;
- Board of the Bank
- Chairman of the Management Board of the Bank;
- Responsible officer for AML/CFT/FPWMD (special official responsible for the work of the bank for the purposes of AML/CFT/FPWMD - head of the Financial Monitoring Department);
- Financial Monitoring Department (UFM);
- Heads of divisions of the Bank;
- Employees of departments involved in banking and other operations and transactions;
- Internal Audit Service (IAS);
- Internal Control Service (ICS).

In order to ensure the implementation of these Rules, the Bank has established an independent structural unit for AML/CFT/FPWMD - FMS, whose competence includes AML/CFT/FPWMD issues. The FMD reports directly to the Chairman of the Management Board of the Bank. The FMD is headed by the Responsible Officer. The structure, tasks, functions and powers of the FMD employees are determined by the Regulations on the FMD, the staff list and job descriptions of employees.

Principles and mechanisms of interaction of system elements:

When interacting, all elements of the AML/CFT/FPWMD system act in the interests of the Bank, exercise their rights and fulfill their obligations in relation to the Bank in good faith and reasonably, within the framework of the current legislation of the Russian Federation and do not use the opportunities provided to them for purposes contrary to Law No. 115-FZ, otherwise regulations in the field of AML/CFT/FPWMD .

The main principles of interaction between the elements of the AML/CFT/FPWMD system are:

The principle of universality is the participation of all elements of the system in countering the legalization (laundering) of proceeds from crime, the financing of terrorism and the financing of the proliferation of weapons of mass destruction. All divisions and employees of the Bank within their competence take part in the implementation of these Rules;

The principle of continuous monitoring is the continuity of internal control for the purposes of AML/CFT/FPWMD . Ensuring constant operational exchange of information between the elements of the system;

The principle of personal responsibility - is expressed in the imposition of responsibility on each employee of the Bank for the performance of the functions assigned to him in the field of AML/CFT/FPWMD ;

The principle of confidentiality is the strict observance by all employees of the Bank of the confidentiality obtained in the AML / CFT process/FROM information and the existence of a ban on informing customers and other persons about the measures taken.

The principle of a multi-level system is a multi-level control system in the Bank. The interaction of the elements of the system is carried out on the basis of compliance with the legislation in the field of AML/CFT/FPWMD and the implementation at each level of the system of measures aimed at identifying transactions subject to mandatory control and transactions containing signs of unusual.

The FMD interacts with the employees of all divisions of the Bank on AML/CFT/FPWMD issues.

Structure, tasks, functions, rights and obligations of employees of the FMD.

In order to ensure the continuity of the implementation of internal control for AML/CFT/FPWMD purposes, the staff of the FMD is 9 people. UFM is headed by the head of UFM– A responsible employee who meets the qualification and business reputation requirements established by applicable law.

A special official responsible for the implementation of the ICR cannot be a person who has an unexpunged or outstanding conviction for crimes in the sphere of the economy or crimes against state power. A special official responsible for the implementation of the Internal Control Rules cannot be a person who does not meet the requirements for business reputation established by law.

The responsible employee is appointed by the Chairman of the Management Board of the Bank and reports directly to the Chairman of the Management Board of the Bank.

The responsible officer of the Bank/the employees of the FMS are independent in their activities from the heads and employees of other divisions of the Bank.

All FMD employees must meet the qualification and business reputation requirements established by law.

The main tasks of the FFM are to ensure:

– taking measures aimed at preventing the legalization (laundering) of proceeds from crime and the financing of terrorism by the Bank's clients

– control over the performance of transactions by the Bank's Clients with cash or other property in order to prevent, detect actions related to the legalization (laundering) of proceeds from crime and the financing of terrorism;

– organization of work (using software tools) to establish information about Clients, Client Representatives, Beneficiaries, Beneficial Owners, about their involvement in extremist activities or terrorism,

– timely communication of updated lists of terrorists/extremists/proliferation of weapons of mass destruction and other negative lists to service units

– confidentiality of information

– organizing training and checking the knowledge of the Bank's employees on AML/CFT/FPWMD .

The main functions of the UFM are:

– consulting Bank employees on issues related to AML/CFT

– ensuring timely sending of messages about operations (transactions) subject to mandatory control or suspicious transactions received from all structural divisions to the authorized body;

– ensuring the receipt of documents from the authorized body, organizing the storage of documents

– assistance to authorized representatives during their inspections of the Bank's activities

– office work and correspondence

The procedure for storing information (documents) obtained (s) as a result of the implementation of AML/CFT/FPWMD policies.

Documents and information obtained in the course of implementing the Internal Control Rules for AML/CFT/FPWMD purposes, incl. received as a result of the initial identification and subsequent study of the Client, are subject to documentary fixation and storage in accordance with the developed procedure.

Documents, content, information about Clients, Representatives, Beneficiaries, Beneficial Owners obtained as a result of the implementation of the Identification Program are stored in the dossier (file) of clients on paper or in electronic form for at least 5 (five) years from the date of termination of relations between the Bank and the Client.

The storage of documents and information is organized in accordance with the internal requirements of the Bank in the field of information security and the Procedure for Ensuring the Confidentiality of Information, which excludes access to them by third parties.

The procedure for participation in the implementation of the Rules of the internal structural divisions of the Bank. Responsibility of officials in the implementation of the Internal Control Rules for the purposes of AML/CFT/FPWMD.

The order of participation in the implementation of the Internal Control Rules for AML/CFT/FPWMD Purposes is that all employees of the internal structural divisions of the Bank, regardless of their position, within the scope of their competence, are obliged to participate in carrying out activities aimed at the implementation of the Internal Control Rules for AML/CFT/FPWMD Purposes.

Employees of the Bank's divisions are responsible for: compliance with the Regulatory Requirements, internal documents of the Bank in terms of identifying Clients, their Representatives, establishing and identifying Beneficiaries, Beneficial Owners, verifying Clients and assigning a degree (level) of risk; completeness and timeliness of detection of transactions subject to mandatory control and suspicious transactions; reliability of information, compliance with the procedure for documenting and storing information; compliance with the established requirements for refusal to open a bank account (deposit) and execution of the Client's order, as well as for compliance with the established requirements for the suspension of operations with cash and other property; timely completion of training events in the field of AML/CFT/FPWMD;

observance of the confidentiality regime and non-disclosure to third parties of information about procedures and confidential information.

The procedure for the interaction of the Bank with subsidiaries, branches and representative offices, as well as members of a group or holding, which includes the Bank.

All programs and policies for the purposes of AML/CFT/FPWMD equally apply to subsidiaries, branches and representative offices, organizations participating in holdings and groups to which the Bank is a member (if any).

The procedure for informing the Bank's employees, including the Responsible Officer, the Chairman of the Management Board of the Bank, the Internal Audit Service and the Internal Control Service of the facts of violation of the Russian Federation legislation in the field of AML/CFT/FPWMD that have become known to them, committed by the Bank's employees.

An important principle of banking activities is the non-involvement of the Bank as a whole and each of its employees in any operations and transactions, as well as in any actions that may raise suspicions of facilitating the legalization (laundering) of proceeds from crime, the financing of terrorism and the financing of proliferation. Weapons of mass destruction.

The facts of complicity (involvement) of employees are a serious violation of official duties and entail the application of disciplinary measures up to and including dismissal, in the manner prescribed by the current labor legislation Russian Federation. Information about such facts, as well as about the facts of any other violations of the AML/CFT/FPWMD legislation, is subject to immediate transfer in writing to the Responsible AML/CFT/FPWMD Officer.

The responsible AML/CFT/FPWMD officer immediately informs the head of the Internal Control Service, the head of the Internal Audit Service, and the Chairman of the Management Board of the Bank about such facts.

3. PROGRAM FOR IDENTIFICATION BY THE BANK OF THE CLIENT, REPRESENTATIVE OF THE CLIENT, BENEFICIARY, BENEFICIAL OWNER

The purpose of the Identification Program for the Client, the Client's Representative, the Beneficiary and the Beneficial Owner is to obtain the information required by law, as well as confirm the accuracy of the information received using original documents and/or duly certified copies.

Employees of the Bank, prior to being accepted for service, are obliged to identify the Clients to whom the Bank provides a service on a one-time basis or whom the Bank accepts for service, assuming a continuing nature of the relationship, as well as to take measures available under the circumstances to identify their Beneficial Owners.

When hiring and servicing Clients, the Bank is obliged to obtain information on the purposes of establishing and the intended nature of their business relations with the Bank, on a regular basis to take reasonable and accessible measures in the circumstances to determine the goals of financial and economic activities, financial position and business reputation of the Clients, and the Bank is also entitled to take reasonable and affordable measures in the circumstances to determine the sources of origin of funds and (or) other property of the Clients.

The nature and extent of these measures are determined taking into account the degree (level) of the risk of suspicious transactions by Clients.

Information about the purpose of establishing and the intended nature of business relations with the Bank, as well as information about the goals of financial and economic activities, financial position and business reputation of Clients - individuals are mandatory established in relation to Clients - individuals with an average and high degree (level) of risk suspicious transactions by the client.

An employee of the Bank establishes information about the goals of the financial and economic activities of the Clients: information about the planned operations on the account during a certain period, the number of operations, the amount of operations, including cash withdrawal operations and operations related to money transfers in the framework of foreign trade activities ; types of agreements (contracts) under which the Client plans to settle through the Bank; the main counterparties of the Client, planned payers and recipients for operations with funds in the account.

The assessment of the financial position and business reputation of the Client is carried out by an employee on the basis of the information and documents received, the results are recorded in the Client's questionnaire. The financial position can be assessed as stable, unstable, business reputation - positive

or negative. In order to determine the sources of origin of funds, the Bank may receive from the Client information or documents confirming the origin of funds.

When performing banking operations and other transactions, an employee of the Bank who directly interacts with the Client is obliged to establish whether the person who applied to the Bank is acting on his own behalf and in the interests or at the expense of another person whose authority is confirmed by documents.

Establishment and identification of Beneficial owners.

The decision to recognize an individual as the Beneficial Owner of the Client is made taking into account the analysis of the totality of documents available to the Bank and (or) information about the Client and such individual - the potential Beneficial Owner, as well as if such person has the ability to control the actions of the Client.

Information about installed as a result of a set of measures described above, the Beneficial owners of the Client are recorded in the forms established by the Bank's internal documents.

The Bank is also obliged to establish whether the Beneficial Owner belongs to the category of a PEP or persons associated with a PEP. In cases where an employee of the Bank establishes or indicates by the Client the ownership Beneficial owner to PEPs, persons associated with PEPs, the Client is assigned an average degree (level) of risk with the appropriate criterion.

Information obtained as a result taking measures to identify the Beneficial Owners are placed in the legal file (dossier) of the Client.

Prior to conducting banking operations and other transactions, an employee of the Bank is obliged to identify the Beneficiary.

In order to identify the Client, his Representative, the Beneficiary and the Beneficial Owner, the Bank's employees collect documents and information required by law. The Clients are obliged to provide the Bank with the information necessary for the fulfillment of the requirements of the Law.

The Bank, in case of failure to identify the Client, the Client's Representative, the Beneficiary and the Beneficial Owner in accordance with the requirements, shall refuse to accept the Client for servicing.

Identification of the Client - an individual, his Representative, Beneficial Owner

In order to identify an individual - a citizen of the Russian Federation, the Bank's employees receive and record the following information: Surname, name and patronymic (if any); Date of Birth; citizenship; details of the identity document, the address of the place of residence or the address of the place of stay; taxpayer identification number; information about the insurance number of the individual personal account of the insured person in the compulsory pension insurance system; Contact Information; belonging to a PEP or persons associated with a PEP.

Identification of the Client - an individual entrepreneur, an individual engaged in private practice in accordance with the procedure established by the legislation of the Russian Federation, his Representative, Beneficial Owner

In order to identify individual entrepreneurs and individuals engaged in the private practice of the Russian Federation in accordance with the procedure established by the legislation of the Russian Federation (hereinafter referred to as the Client-individual entrepreneur), the Bank establishes the following information: information obtained in order to identify an individual; information on registration as an individual entrepreneur: date of registration, state registration number, name of the registering authority, place of registration; Domain name, site page index on the Internet, with the use of which the Client-individual entrepreneur provides services (if any); information on licenses for the right to carry out activities subject to licensing; Contact Information; belonging to a PEP or persons associated with a PEP; information about the purpose of establishing and the intended nature of business relations with the Bank, information about the goals of financial and economic activities; information about business reputation; information about the financial situation; information about the sources of origin of funds and (or) other property.

Identification of the Client - a legal entity, a foreign structure without forming a legal entity

In order to identify a legal entity - a resident of the Russian Federation, the Bank establishes the following information: name, company name in Russian and in foreign languages; organizational and legal form; taxpayer identification number; information on state registration: main state registration number, place of state registration (location); legal entity address; information on licenses for the right to carry out activities subject to licensing (if any); domain name, index of the site page on the Internet, with the use of which services are provided by the legal entity (if any); information about the bodies of the legal entity (the structure and personnel of the management bodies of the legal entity, with the exception of information on the personal composition of shareholders (participants) of a legal entity owning less than five percent of the shares (stakes) of a legal entity); Contact Information.

In order to identify a legal entity - a non-resident of the Russian Federation, the Bank additionally establishes the following information:
taxpayer identification number or code of a foreign organization; number of an entry on accreditation of a branch, representative office of a foreign legal entity in the state register of accredited branches, representative offices of foreign legal entities, registration number of a legal entity at the place of establishment and registration; the address of the legal entity in the territory of the state in which it is registered;

The Bank takes reasonable and affordable measures in the circumstances to identify the Beneficial Owners

The decision to recognize an individual as the Beneficial Owner of the Client is made taking into account the analysis of the totality of documents and (or) information available to the Bank about the Client, about such an individual - a potential Beneficial Owner, and also if such a person has the ability to control the actions of the Client

Peculiarities of identification when establishing correspondent relations with other credit institutions that are not foreign banks.

When establishing correspondent relations with a resident bank, the Bank requests from it information and copies of documents confirming them, obtained for the purpose of identification according to the Questionnaire for credit institutions, as well as information on measures taken by the resident bank to counter the legalization (laundering) of proceeds from crime. way, and the financing of terrorism.

The Bank has the right to request the following information: balance and calculation of standards as of the last reporting date; copy of the last annual balance sheet and auditor's report; list of correspondent banks; certified copies of confirmations on the approval of the persons indicated in the card in the territorial office of the Bank of Russia.

When establishing and maintaining correspondent relations with credit institutions that are not foreign banks, the Bank takes into account the following recommendations:

- apply due diligence measures in full, it is unacceptable to apply simplified measures when conducting such an audit;
- conduct a comprehensive assessment of all the risk factors that characterize it, as well as the level of effectiveness of their own measures to reduce the risks taken;
- take measures to establish a management and ownership structure;
- evaluate the applied AML/CFT/FPWMD measures;
- set out how the account is to be used, including whether third parties (i.e., the respondent's clients and those to whom the respondent provides correspondent banking services) can access the account;
- when determining approaches to monitoring transactions, take into account the level of risk, existing cases of failure to provide information at the request of the Bank, as well as the type of transactions for which a correspondent account is opened;
- The result of monitoring operations may be sending a request for additional information about a specific operation and, if necessary, about the client on whose behalf it was carried out.

When the counterparty bank provides the required information and documents, the Bank examines the submitted data and checks their sufficiency for identification purposes.

If Russian credit institutions provide false information, provide incomplete information, or if the Bank considers the AML/CFT/FPWMD measures taken by the counterparty bank to be unsatisfactory, the Bank has the right to refuse to establish correspondent relations, conclude transactions, contracts, master agreements establishing other relationships.

Peculiarities of carrying out identification when establishing correspondent relations with foreign banks.

When establishing correspondent relations with a non-resident bank, the Bank requests from it information and copies of documents confirming them, received for identification purposesaccording to the Questionnaire for credit institutions, as well as information on the measures taken by the non-resident bank to counter the legalization (laundering) of proceeds from crime and the financing of terrorism.

When establishing and maintaining correspondent relations with foreign banks, the Bank takes into account the following recommendations:

When establishing correspondent relations with a non-resident bank, the Bank checks the presence of the country of registration and location of the non-resident bank in the Lists of states and territories that provide preferential tax treatment and (or) do not provide for the disclosure and provision of information, the Lists of states that pose a threat to the global financial system, the Lists states that finance or support terrorist activities, the List of foreign states or territories known from international sources to be states or territories with a high level of corruption, as well as states in which narcotic substances are illegally produced or through which drugs are trafficked, compiled on the basis of information obtained from official sources and relevant to the current date.

If the country of location coincides with the above lists, the Bank assesses the risk of establishing correspondent relations with a non-resident bank, requests additional information and documents in accordance with regulatory legal acts, and decides on the possibility of establishing correspondent relations.

The Bank is not entitled to establish and maintain relations with non-resident banks that do not have permanent management bodies in the territories of the states in which they are registered.

Prior to establishing relations with non-resident Banks, the Bank's employees are required to make sure that the given Bank has permanent governing bodies in the territory of the state in which it is registered. The Bank is prohibited from establishing and maintaining relations with non-resident banks that do not have permanent management bodies in the territories of the states in which they are registered.

Measures aimed at identifying PEPs. The procedure for accepting PEPs for service.

Employees of subdivisions are obliged to take reasonable and accessible measures in the circumstances to identify among individuals who are in service or accepted for service public officials belonging to the categories of foreign public officials, international public officials, Russian public officials. (hereinafter, when jointly referred to as PEP).

The Bank places the necessary visual information in customer service points accessible to customers in order to inform about the need to take measures to comply with the requirements of Article 7.3. Federal Law 115-FZ.

In order to identify public officials, the Bank uses the following methods: questioning (filling out a questionnaire according to the forms; oral questioning; checking against commercial lists, etc.)

Identification of PEPs is carried out regardless of the citizenship of the person being or accepted for service. Measures to identify PEPs are carried out in relation to individuals who are under service or accepted for service, including when performing one-time transactions, with the information received entered into the Bank's ABS.

The Bank accepts PEPs for servicing only on the basis of a written decision of the Chairman of the Management Board of the Bank or his deputy.

Service for PEPs

Employees serving clients - individuals who are PEPs, or legal entities, representatives, beneficiaries, beneficial owners, whose founders are PEPs, regularly monitor the transactions of this client. Monitoring of operations of clients - legal entities is carried out by an employee serving the client, at least once a month. Monitoring of operations of clients - individuals is carried out during operations.

In case of doubts about the reliability of the information provided by the client, as well as in case of suspicion that the operation is carried out for the purpose of legalization (laundering) of proceeds from crime or financing of terrorism, an employee of the Financial Monitoring Department, through an employee serving the client, requests documents confirming the source of origin of funds or other property.

Employees of the Units are obliged to take reasonable and affordable measures in the circumstances to identify among the persons accepted and / or in service, spouses, close relatives (relatives in the direct ascending and descending line (parents and children, grandparents and grandchildren), full and half-blooded (having a common father or mother) brothers and sisters, adoptive parents and adopted children) of PEPs or persons acting on their behalf (hereinafter referred to as persons associated with PEPs). The specified information can be obtained by oral questioning of the Client or by collecting information in accordance with the forms of documents approved by the Bank.

Employees of subdivisions should pay increased attention to transactions with funds or other property carried out by PEPs serviced by the Bank, persons associated with PEPs, as well as on a regular basis to update the available information on PEPs and persons associated with PEPs in the Bank's service

The Bank is obliged to take reasonable and affordable measures in the circumstances to determine the sources of origin of funds or other property of foreign PEPs, to update on a regular basis the information available to the Bank about foreign PEPs being serviced.

Requirements for documents and information received for identification purposes.

Documents and information on the basis of which the identification of the Client, the Client's Representative, the Beneficiary, the Beneficial Owner is carried out, must be valid on the date of their presentation (receipt).

Documents drawn up in full or in any part in a foreign language (with the exception of documents proving the identity of individuals issued by the competent authorities of foreign states, drawn up in several languages, including Russian), are submitted to the Bank with a duly certified translation into Russian .

The procedure for updating information about Clients, Beneficiaries and Beneficial Owners.

The Bank updates the information obtained as a result of the identification of Clients, Client Representatives, Beneficiaries, Beneficial Owners within the time limits established by Law No. 115-FZ, as well as update the assessment of the degree (level) of the risk of suspicious transactions by the client.

When servicing clients and updating information about them, the Bank applies the “Know Your Client” principle and a risk-based approach.

The Bank is obliged to update the specified information on clients (their representatives, beneficiaries, beneficial owners) who are classified as a low degree (level) risk of suspicious transactions - at least once every three years, and in case of doubts about the reliability and accuracy of the previously received information within seven working days following the day of the occurrence of these doubts. Information on clients (their representatives, beneficiaries, beneficial owners) who are not classified as a low degree (level) risk of suspicious transactions is updated at least once a year, and in case of doubts about the reliability and accuracy of previously received information within seven working days following the day of the occurrence of these doubts;

The fact of updating the information is recorded by putting down the date of updating in the Client's Questionnaire.

If the Client fails to provide the documents and information necessary to complete the update of information, in particular documents confirming the change in the information available, the Bank has the right to exercise the right to refuse the Client to accept instructions from him to conduct transactions on a bank account (deposit), signed a handwritten signature tax.

The procedure for assessing the degree (level) of the risk of the Client making suspicious transactions, the basis for assessing such a risk.

The assessment of the degree (level) of the risk of the client making suspicious transactions is carried out at the stage of acceptance for service, identification, as well as when servicing the Client, and

is the result of an analysis of the Bank's documents, information and information about the Client and his activities based on the factors recorded in the Questionnaire.
The assessment of the degree (level) of the risk of committing suspicious transactions by the client is carried out at three levels - low, medium and high.
The assessment of the degree (level) of the risk of the client committing suspicious transactions is carried out by assigning a final assessment of the risk level for the totality of the following risk categories:

- the risk by type of the Client and/or the Beneficial Owner is assessed upon acceptance of the Client for servicing and is reviewed at the time of the renewal deadline in accordance with the deadline established by Law No. 115-FZ. The risk is reviewed immediately, but no later than the next business day, when factors affecting the assessment of the level (degree) of the risk of the client making suspicious transactions are identified at the “high” level;

- country risk is assessed when establishing relations with the Client and is reviewed at the time of the renewal deadline in accordance with the deadline established by Law No. 115-FZ;

- the risk associated with the commission (implementation) by the Client of a certain type of transactions and (or) activities is assessed and reviewed at the time of the renewal deadline in accordance with the deadline established by Law No. 115-FZ. The risk is reviewed immediately, but no later than the next business day, when the factors affecting the assessment of the level (degree) of the risk of suspicious transactions by the client at the “high” level are established.

4. PROGRAM TO IDENTIFY PERSONS UNDER SANCTIONS (SANCTIONS COMPLIANCE) AND COMPLIANCE WITH FOREIGN TAXPAYERS

Sanctions compliance.

The Bank constantly complies with international and national sanctions, in the manner and to the extent prescribed by regulatory enactments. The control of sanctions lists is carried out in accordance with the internal policy, which determines the goals, distribution of powers and rules for the implementation of controls.

The Bank comprehensively analyzes its customers and their operations in order to prevent the Bank from being used to conclude transactions and conduct illegal operations and operations, the implementation of which may violate legal norms and requirements, and is also associated with high reputational, geopolitical and other risks.

The Bank has implemented automated procedures aimed at ensuring compliance by the parties involved with the relevant sanctions programs, as well as legal requirements. In particular, a constant updating of the lists and comparison of the client base and counterparties of clients according to the following lists of sanctions has been implemented:
US OFAC Sanctions List, Switzerland SECO Sanctions List, Europe EU Sanctions List, UK HM Treasury Sanctions List, Ukraine MEDT Sanctions List, US BISN Sanctions List, Canada SEMA Sanctions List, Australia DFAT Sanctions List, South Africa FIC Sanctions List, UAE UAE Sanctions List (UN List), Singapore MAS Sanctions List (UN List), Hong Kong HKMA Sanctions List (UN List), UAE UAE Terrorists Sanctions List, Singapore MAS TSFA Sanctions List, UN UN Sanctions List, Japan JMOFJ Sanctions List, Japan JMETI Sanctions List, Sanctions List China Pbc (UN List), Sanctions List Kazakhstan KFM (UN List), Sanctions List Kazakhstan KFM Local, Sanctions List Kazakhstan KFM Int, Sanctions List Azerbaijan AZFMS Int, Sanctions List Azerbaijan AZFMS Local,Georgia GEGOV Sanctions List, Germany DBB Sanctions List (UN List), Germany DBB Sanctions List (EU List), Spain SMFA Sanctions List (UN List), Spain SMFA Sanctions List (EU List), Luxembourg CSSF Sanctions List (UN List), Luxembourg CSSF (EU List), Gibraltar GFIU Sanctions List, France GEL Sanctions List, Belgium FOJ Sanctions List, JFSC Jersey Sanctions List (HMT List), JFSC Jersey Sanctions List (EU List), JFSC Terrorists Jersey Sanctions List, JFSC Terrorists Sanctions List Latvia LVSCS (UN List), Sanctions List Latvia LVSCS (EU List), Sanctions List Latvia LVSCS National, Sanctions List Malta MFSA (UN List), Sanctions List Malta MFSA (EU List), Sanctions List Malta MFSA (OFAC List), Sanctions list Monaco SICCFIN NL,Monaco Sanctions List SICCFIN (UN List), Netherlands Sanctions List NNTS (UN List), Netherlands Sanctions List NNTS (EU List), Netherlands Sanctions List NNTS Terrorists, Lebanon Sanctions List LBISF (UN List), Lebanon

Sanctions List LBISF Local, Sanctions List Taiwan TWMOJ (UN List), Taiwan TWMOJ Sanctions List, US CCMC-CMIC Sanctions List, Israel IMOD WMD Sanctions List, Israel IMOD TL Sanctions List, US BIS Sanctions List, US DDTC Sanctions List, US CAATSA Sanctions List, UK PTOL Sanctions List , Sanctions List Russia PP1300, Sanctions List Europe EUASL, Sanctions List USA BEBA (OFAC List), Sanctions List USA BEBA (BIS List), Sanctions List Europe EU Manual, Sanctions List UK UKSL, Sanctions List Poland MWSIA, Sanctions List Russia RUS851, Sanctions List Japan MOFA, Sanctions List New Zealand MFAT (UN List), Sanctions List New Zealand MFAT RUSSIA.

The Bank controls both a direct match with the sanctions lists, and match according to the "50%" participation rule.

Taking into account the direction and nature of international sanctions, the Bank has the right to refuse the client to perform a transaction if there are sufficient grounds that international sanctions apply to the relevant transaction and/or to one of its participants. The Bank has the right to terminate cooperation with clients who are subject to sanctions or have been seen in violation or circumvention of sanctions.

Identification of foreign taxpayers and reporting on foreign taxpayers.

In accordance with the requirements of Federal Laws No. 173 dated June 28, 2014, No. 340 dated November 27, 2017, Government Decree No. 693 dated June 16, 2018, the Bank takes measures to identify among customers who enter into (have entered into) an agreement with the Bank providing for the provision of financial services, persons who are subject to the legislation of a foreign state on the taxation of foreign accounts (FATCA / CRS).

The Bank carries out identification in order to determine the tax residence of clients, beneficiaries, as well as persons directly or indirectly controlling the client, according to the established forms of certification (self-certification).

Information about foreign taxpayers is included in the annual reporting and sent to the relevant tax authorities within the time limits specified by law.

If the client refuses to provide the information requested by the Bank for the identification procedure in order to determine tax residency, the Bank has the right to refuse such a client to conclude an agreement providing for the provision of financial services, on the basis of clause 4 of Art. 142.4 Chapter 20.1 of the Tax Code of the Russian Federation.

5. RISK MANAGEMENT PROGRAMME FOR MONEY LAUNDERING, TERRORIST FINANCING AND THE FINANCING OF PROLIFERATION OF WEAPONS OF MASS DESTRUCTION

Organization of a risk management system for the legalization (laundering) of proceeds from crime, the financing of terrorism and the financing of the proliferation of weapons of mass destruction.

For the purposes of this Program, managing the risk of legalization (laundering) of proceeds from crime and the financing of terrorism and financing the proliferation of weapons of mass destruction should be understood as a set of actions taken by the Bank aimed at assessing such a risk and minimizing it by taking measures provided for by law, such as: request from Clients and analysis of documents for compliance with the information available to the Bank, refusal to perform a transaction, refusal to conclude a bank account agreement, terminate a bank account agreement, analysis of the client's counterparties and the client's ownership structure, blocking a bank card, holding a conversation with a client, sending recommendations on the termination or reduction of the volume of transactions arousing the Bank's suspicions, other methods. Risk management is carried out by the Bank on the basis of a risk-based approach that allows the application of AML/CFT/FPWMD measures that are commensurate with the assessed risk.

The structure of the system for assessing the Bank's activities in terms of risk levels of legalization (laundering) of proceeds from crime, financing of terrorism and financing of the proliferation of weapons of mass destruction includes the following types of risks:

- the risk of the Client making suspicious transactions
- the risk of involvement of the Bank and its employees in the use of the Bank's services for the purpose of legalization (laundering) of proceeds from crime, financing of terrorism and financing the proliferation of weapons of mass destruction (hereinafter referred to as the product/service risk).

When accepting and servicing Clients, the Bank assesses the degree (level) of the risk of committing suspicious transactions by them, including taking into account the results of the national risk assessment, the nature and types of their activities, the nature of the products (services) they use, provided by the Bank, and classifies each Client to the risk group for suspicious transactions, depending on the degree (level) of the risk of suspicious transactions by the Client.

The Bank assigns each Client to one of the three risk groups for suspicious transactions (hereinafter referred to as the "risk group") depending on the following degrees (levels) of the risk of making suspicious transactions (hereinafter referred to as the degree (level) of risk for the client to perform suspicious transactions):

low degree (level) of risk of the client making suspicious transactions;

the average degree (level) of the risk of the client making suspicious transactions;

a high degree (level) of the risk of the client making suspicious transactions.

The risk of the product / service considered in this Program is assessed on a two-level risk scale, which includes low and high risk levels.

The main objective of the Risk Management Program is to classify Clients and areas of the Bank's activities (products and/or services provided to Clients) by risk levels in order to concentrate efforts on areas subject to the highest level of risk. In order to manage the AML/CFT/FPWMD risk, the Bank's divisions need to carry out the following procedures: risk identification, including identification and assessment of the degree (level) of the risk; measures to prevent the realization (minimization) of the risk.

These measures are applied by the Divisions depending on the assessment of the degree (level) of the risk of the client performing suspicious transactions and the level of risk of the product and/or service provided.

Peculiarities of monitoring and analysis of customer transactions relating to different degrees (levels) of risk.

With regard to Clients who are assigned a “low” degree (level) of risk, standard control procedures are applied, provided for by the regulatory documents of the Bank of Russia, including: Client information is updated as Client information is submitted, but at least once every three of the year; other measures, the composition of which is determined based on the circumstances of the Client's activities and the nature of banking services provided to the Client.

In relation to the Clients who are set to the "medium" degree (level) of risk, measures are taken to reduce the risk of the Client making suspicious transactions in accordance with the current legislation of the Russian Federation and in the manner established by the Bank, including: the information about the Client is updated as information is provided by the Client, his Representative, but at least once a year; carrying out, if necessary, an in-depth audit of the Client's activities in accordance with The procedure for checking information about Clients; after conducting an in-depth check, it is possible to restrict the provision of banking products/services to the Client that carry an increased risk, including the suspension of the provision of remote banking services, etc.; refusal to further provide the Client with new banking services (if this is allowed by their nature); holding a meeting with the founders, beneficial owners, the sole management body of the Client, other representatives of the Client; carrying out an additional field check of the presence of the Client at the place of its location (registration) in the manner established by the Bank; refusal to perform the operation; termination of the bank account agreement; other measures, the composition of which is determined based on the circumstances of the Client's activities and the nature of banking services provided to the Client.

In relation to the Clients who are assigned a “high” degree (level) of the risk of committing suspicious transactions (actions), measures of increased attention are applied in accordance with the current legislation of the Russian Federation and in the manner established by the Bank, including: in relation to clients who are assigned an "average" degree (level) of risk; restriction of the provision of banking products/services to the Client, including refusal to provide the Client with remote banking services, blocking of bank cards; measures aimed at terminating the relationship with the client; other measures, the composition of which is determined based on the circumstances of the Client's activities and the nature of banking services provided to the Client.

A methodology for identifying and assessing the risk of legalization (laundering) of proceeds from crime, the financing of terrorism and the financing of the proliferation of weapons of mass destruction in relation to the risk of a product / service.

The degree (level) of the risk of involvement of the Bank and its employees in the legalization (laundering) of proceeds from crime and the financing of terrorism (product/service risk) is assessed by the FMD based on the risk of using certain types of products/services by Clients, as well as taking into account the specifics of the business -processes, level of automation and maturity of control procedures in departments. The factor (risk level criterion) that influences the risk assessment is the FMD's expert opinion on the risk of the product/service.

The procedure for assigning a degree (level) of risk to a product/service, the procedure for monitoring, analyzing and controlling the risk of a product/service.

The risk of a product/service is identified and documented by the Responsible Officer by analyzing and assessing the level of risk of existing products/services in the following order: for existing products/services - quarterly or within the period established by the executive act of the Chairman of the Management Board of the Bank, but at least once at six months;

In order to assess (review) the level of risk of a product/service, the divisions whose competence includes the development, implementation and maintenance of banking products/services and (or) software and hardware tools that enable Clients to perform transactions with cash or other property are obliged to the beginning of the provision of the specified products/services and (or) software and hardware to the Clients, to agree on their main parameters and the procedure for providing them with the FMS.

Before providing new services and (or) software and hardware tools that enable clients to perform transactions with money or other property, the Bank is obliged to assess the possibility of using such services and (or) software and hardware tools for the purpose of legalizing (laundering) the proceeds of crime. through and financing of terrorism and, based on the results of this assessment, take measures aimed at reducing (minimizing) this possibility.

Product/service risk control is exercised and documented in relation to the following transactions: cash withdrawal transactions, cash deposit transactions, transactions with securities, money transfers without opening a bank account, operations for certain international settlements.

Based on the analysis of the risk assessment system, if there are grounds for revising the factors of the level (degree) of the risk of the client performing suspicious transactions or the level of risk of the product/service, the Responsible employee of the Bank takes measures to revise them, aimed at bringing the Bank's risk assessment system in line with the specifics of the client's base, the nature of the products (services) provided to the Clients, as well as with current changes in the typologies of the legalization (laundering) of proceeds from crime and the financing of terrorism. The Bank pays special attention to operations (transactions) carried out by a PEP or a person related to a PEP.

6. A PROGRAMME FOR IDENTIFICATION OF CUSTOMER TRANSACTIONS SUBJECT TO MANDATORY CONTROL AND TRANSACTIONS SUSPECTED OF BEING CONDUCTED FOR THE PURPOSE OF MONEY LAUNDERING, TERRORIST FINANCING AND THE FINANCING OF PROLIFERATION OF WEAPONS OF MASS DESTRUCTION, A SET OF SUSPICIOUS TRANSACTIONS AND (OR) ACTIVITIES

The purpose of the Program is to identify transactions in the activities of Clients that are subject to mandatory control, and transactions in respect of which there are suspicions that they are carried out for the purpose of legalizing (laundering) proceeds from crime, financing terrorism or financing the proliferation of weapons of mass destruction, a combination of suspicious transactions and (or) actions are the identification, documenting and sending to the authorized body of information:
on the operations of the Clients provided for inparagraphs 1-1.4,1.6-1.9,2 articles 6,paragraph 6 of article 7.4Andparagraph 1 of article 7.5Law No. 115-FZ no later than 3 (three) business days following the day of the transaction. Transactions are identified in accordance with the procedure established by the Bank on the basis of the criteria specified in the current legislation.

In the event that the employees of the Bank, based on the implementation of internal regulatory documents, have suspicions that any one-time operation or a set of operations and (or) actions of the Client related to the conduct of any operations, his representative within the framework of servicing the Client, are carried out in for the purpose of legalization (laundering) of proceeds from crime or financing of terrorism, the Bank sends information about suspicious transactions and (or) suspicious activity no later than 3 (three) business days following detection such transactions and/or suspicious activity.

Distribution of responsibilities between departments.

In the process of implementing the Operations Identification Program, all employees of the departments within their competence are required to participate before the start of operations, in the process of performing them, in case of refusal to perform them. Heads of departments organize the work of their employees to identify transactions subject to mandatory control and suspicious transactions, as well as to generate and timely send to the FMD information to be sent to the Authorized Body, and are personally responsible for the quality of such work in the departments they lead.

Operations are detected automatically and manually.

The FMD is responsible for setting up the software, collecting information and sending information to be sent to the Authorized Body.

The FMS establishes the procedure for preparing, generating and sending information to the Authorized Body, identifies and analyzes transactions subject to mandatory control and suspicious transactions carried out by the Bank's Clients in an automated mode using a software product, consolidates messages received from departments, and exercises output (logical) control and uploading files of the consolidated report, ensures the timely sending of messages on transactions subject to mandatory control, suspicious transactions, suspicious activities to the authorized body, ensures the receipt of documents from the authorized body.

The responsible officer has the right to establish additional signs of suspicious transactions, as well as the execution parameters characteristic of suspicious transactions - amount thresholds, time periods and other features that indicate unusualness.

Signs of unusual transactions are indicated in internal regulations and are not exhaustive. A transaction may also be recognized as suspicious based on an analysis of the nature of the transaction, its components, the circumstances accompanying it and interaction with the Client, even if the transaction formally does not correspond to any of the signs.

The procedure for conducting an in-depth check of documents and information about the Client, his operation and his activities in order to confirm the validity or refute the suspicions that have arisen regarding the Client's operation.

An in-depth check of documents and information about the Client or the Client’s operation is carried out in order to confirm the validity or refute the suspicions arising from the employees of the divisions that the Client’s activities or the operation being carried out are related to the legalization (laundering) of proceeds from crime and the financing of terrorism.

If the employee servicing the Client's account, during the processing of documents, has a suspicion that the operation is being carried out for the purpose of legalizing (laundering) proceeds from crime, he reports his suspicions to the Responsible Officer by sending a message.

The responsible officer decides on the further actions of the Bank in relation to the Client and his transaction. Solutions can be as follows:

- analyze the Client's operations for the period of time preceding the detection of a suspicious transaction (the period is determined taking into account the specifics of the Client's activities and the number of transactions performed);
- review the degree (level) of risk to the Client and organize increased attention to all operations (transactions) of the Client conducted through the Bank;
- contact the client with a request (in writing or orally) to provide the necessary explanations, additional information explaining the economic meaning of the suspicious transaction;
- request documents that allow assessing the adequacy of the declared scope and results of economic activity to the volume of operations carried out by the Clients through accounts opened with the Bank (balance sheets, financial results reports, income tax and VAT tax returns with a tax authorities' mark of receipt, staffing tables and etc.);
- carry out other actions subject to compliance with the legislation of the Russian Federation.

The term for verifying information to confirm the reasonableness of suspicions and making a decision on qualifying the Client's transaction as suspicious should not exceed 10 (ten) business days from the date of discovery in the Client's activities of an operation / transaction in respect of which the Bank has a suspicion that it is carried out for the purpose of legalization (laundering) proceeds from crime and/or financing of terrorism. If it is necessary and expedient to request additional information, the specified period, based on the decision of the Responsible Officer of the Bank, may be extended for the period necessary for additional study. An additional period is established in each case at the discretion of the Responsible Officer. The date of detection of a suspicious transaction is the date when the Responsible Officer makes the final decision to recognize the transaction as suspicious based on a reasoned judgment. For the duration of the audit, by decision of the Responsible Officer of the Bank, the client may be suspended access to remote service channels.

Information about transactions in respect of which the reasonableness of suspicions of legalization (laundering) of proceeds from crime by the Client is confirmed is sent to the authorized body no later than three days following the day the relevant decision is made.

Based on the results of the in-depth due diligence of the Client and on the basis of a reasoned judgment, the Head of the Division takes reasonable and available measures in the circumstances to limit the involvement of the Bank in illegal activities in accordance with the procedure set forth inrisk management program.

7. THE PROGRAM OF ORGANIZING WORK IN THE BANK ON REFUSAL TO CONCLUDING A BANK ACCOUNT (DEPOSITION) AGREEMENT, REFUSAL TO PERFORM AN OPERATION, AND TO TERMINATE A BANK ACCOUNT (DEPOSITION) AGREEMENT

Grounds for refusal to conclude a bank account (deposit) agreement with the Client.

The Bank's divisions, whose competence includes the conclusion of bank account (deposit) agreements with a client, are prohibited from:

- establish and maintain relations with non-resident banks that do not have permanent management bodies in the territories of the states in which they are registered;
- open and maintain accounts (deposits) for anonymous owners, that is, without providing the account (deposit) opening individual or legal entity, a foreign structure without forming a legal entity, documents and information necessary for its identification, as well as open and maintain accounts (deposits) on owners using fictitious names (pseudonyms);
- open accounts (deposits) for Clients without the personal presence of the individual opening the account (deposit) or the Client's Representative, except as provided by Law No. 115-FZ;
- conclude bank deposit (deposit) agreements with execution of documents certifying the deposit (deposit) to bearer;
- to accept for servicing persons carrying out activities on the territory of the Russian Federation without a license obtained in accordance with the established procedure, if legislation The Russian Federation in relation to such activity provides for its existence, as well as to carry out operations

with funds or other property on behalf of such persons.

- accept for servicing, as well as carry out transactions with funds and other property on behalf of persons providing services using a site on the Internet, if the domain name of this site, the page index of this site are contained in the Unified registry domain names, pointers to pages of sites on the Internet and network addresses that make it possible to identify sites on the Internet that contain information whose distribution is prohibited in the Russian Federation.

The Bank's divisions, whose competence includes the conclusion of bank account (deposit) agreements with Clients, including credit institutions, have the right to refuse to conclude a bank account (deposit) agreement with a Client if there are suspicions that the purpose of concluding such an agreement is to perform operations for the purpose of legalization (laundering) of proceeds from crime, financing of terrorism and financing of the proliferation of weapons of mass destruction.

Refusal to perform a transaction.

The bank is obliged to refuse to execute the order of the payer in the absence of complete information about the payer in the settlement or document. The decision to refuse to perform the operation in this case is entitled to be taken by the immediate supervisor of the employee who has revealed the absence of the necessary information about the payer in the settlement or other document.

The Bank is obliged to refuse to conduct a transaction with funds and / or other property, one of the parties to which is a foreign or international non-governmental organization included in the list of foreign and international non-governmental organizations whose activities are recognized as undesirable on the territory of the Russian Federation.

The decision to refuse to conduct a client operation in this case is entitled to be taken by the immediate supervisor of the employee who revealed the above operation.

The Bank has the right to refuse to perform a transaction, provided that, as a result of the implementation of the Rules, the employees of the divisions have suspicions that the transaction is being carried out in order to legalize (launder) proceeds from crime, finance terrorism and finance the proliferation of weapons of mass destruction.

The procedure for informing the Client about the decision taken by the Bank regarding him to refuse to perform the operation.

In case of refusal to perform a transaction or to open an account (deposit), the Bank shall provide information on the date and reasons for the decision to refuse to complete the transaction in writing no later than five business days from the date of the relevant decision to refuse.

Termination of the bank account (deposit) agreement with the Client.

The Bank shall have the right to terminate the bank account (deposit) agreement with the Client in the event that within a calendar year 2 (two) or more decisions are made to refuse to perform a transaction on the basis of the client's order in the case provided forparagraph11 article 7 of Law No. 115-FZ.

8. THE PROGRAM DETERMINING THE PROCEDURE FOR APPLICATION OF MEASURES TO FREEZE (BLOCKING) THE CUSTOMER'S CASH OR OTHER PROPERTY AND THE PROCEDURE FOR VERIFICATION OF THE AVAILABILITY OF ORGANIZATIONS AND INDIVIDUALS AMONG THEIR CLIENTS TO WHICH ARE APPLIED OR MEASURES TO FREEZE (BLOCK) CASH OR OTHER PROPERTY MUST BE APPLIED

The Bank takes measures to freeze (block) funds or other property of the Clients immediately, but no later than one business day from the date of posting on the Internet on the official website of the Authorized Body of information on the inclusion of an organization or individual in the list of organizations and individuals, in relation to who have information about their involvement in extremist activities or terrorism, or in the List of persons involved in the PF, or from the date of posting on the Internet on the official website of the authorized body of the decision to apply measures to freeze (block) funds or other property belonging to the organization or an individual in respect of whom there are reasonable grounds to suspect their involvement in terrorist activities (incl.financing of terrorism) in the

absence of grounds for inclusion in these lists, immediately informing the authorized body of the measures taken.

The Bank also applies measures to freeze (block) funds or other property immediately, but no later than one business day from the date of posting on the Internet on the official website of the authorized body of the decision to freeze (blocking) of funds or other property, informing the authorized body of the measures taken immediately, but no later than one working day following the day of application of the said freezing (blocking) measures.

The Bank at least once every three months checks the presence among its customers of organizations and individuals in respect of which measures have been applied or should be applied to freeze (block) funds or other property in accordance, and inform on the results of such an audit, the authorized body.

The Bank cancels the measures applied to freeze (block) funds or other property immediately, but no later than one business day from the date of posting on the Internet on the official website of the authorized body of information about the exclusion of an organization or individual from the list of organizations and individuals in respect of which there is information about their involvement in extremist activities or terrorism.

The procedure for obtaining information posted on the official website of the authorized body on the Internet, comparing lists with the client base, notifying the authorized body

Employees of the FMD daily monitor the updating of the List of extremists, the List of the Interregional Commission, the List of persons involved in the PF, posted on the official website of the Authorized Body on the Internet (http://www.fedsfm.ru/).

Employees of the FMD receive the above information posted on the Internet on the official website of the Authorized Body, as well as information on the partial or complete cancellation of the measures applied to freeze (block) funds or other property in accordance with clauses 2.5. article 6, paragraph 7 of article 7.5. Law No. 115-FZ, using the Personal Account on the official website of the Authorized Body.

At least once every three months, FMD employees are required to check the presence among the Clients of organizations and individuals in respect of which measures have been or should be applied to freeze (block) funds or other property.

Upon receipt of a new List of extremists, the List of the IAC, as well as the List of persons involved in the PF, in the manner prescribed by paragraph 10.1.3., employees of the FMD immediately, but no later than one business day from the date of posting on the Internet on the official website of the Authorized Information Agency about the inclusion of an organization or an individual in the specified List, they check for the presence among their Clients of organizations and individuals in respect of which measures have been or should be applied to freeze (block) funds or other property.

Immediately, on the day of application of measures to freeze (block) the funds or other property of the Client, the employees of the FMS inform the Authorized Body about the measures taken to freeze (block) the funds or other property of the Client.

All cases of freezing (blocking) of funds or other property of the Clients, as well as information on the cancellation of measures are recorded by the employees of the FMS in the register of such information in the form established by the Bank.

The head of the Bank's subdivision stores documents and information generated as a result of the implementation of this Program in accordance with Information storage order (documents).

9. AML/CFT/FPWMD TRAINING AND TRAINING PROGRAM IN THE BANK

The AML/CFT/FPWMD training program for personnel at the Bank (hereinafter referred to as the AML/CFT/FPWMD training program) is developed taking into account the requirements of the legislation, as well as the specifics of the Bank’s activities, the specifics of the activities of its clients and the degree (level) of risk of transactions performed by clients for the purpose of legalization (laundering) of proceeds from crime, financing of terrorism and financing of the proliferation of weapons of mass destruction.

The purpose of AML/CFT/FPWMD training for Bank employees is to obtain AML/CFT/FPWMD knowledge necessary for them to comply with regulatory legal and other acts of the Russian Federation in the field of AML/CFT/FPWMD and internal documents of the Bank on AML/CFT/FPWMD .

Responsible for the implementation of the AML/CFT/FPWMD Training Program, organization and conduct of training events and knowledge tests are: the head of the Training Center, responsible employees of the FIM, heads of the Bank's divisions.

Training activities, knowledge testing can be carried out individually or in groups, in the form of a seminar, a distance course on the Portal of the Learning Center, sending material by e-mail. Knowledge testing can be carried out individually or in groups, in the form of an interview or testing, including remotely through the Portal of the Learning Center.

The training is conducted in accordance with the implementation plan of the AML/CFT/FPWMD Training Program for the current year (hereinafter referred to as the Plan). The plan includes the topics of training events, the timing of their implementation and the persons responsible for conducting the training. The plan is approved by the Chairman of the Board of the Bank no later than February 15 of the current year. During the year, changes and additions may be made to the Plan, which are approved by the Chairman of the Management Board of the Bank.

Procedure for training the Bank's employees.

The responsible officer conducts an introductory (primary) briefing and familiarization with the regulatory legal and other acts of the Russian Federation in the field of AML/CFT/FPWMD and the Bank's internal documents on AML/CFT/FPWMD when hiring employees to work in the units included in the List, as well as when transfer to work in the specified divisions of employees of other divisions of the Bank.

Target(unscheduled) briefing of employees of the Bank's divisions included in the List of divisions is carried out in the course of their work in the following cases:

- in case of changes in existing and entry into force of new regulatory legal and other acts of the Russian Federation in the field of AML/CFT/FPWMD ;
- when the Bank introduces new or changes to existing internal control rules for AML/CFT/FPWMD purposes and programs for its implementation;
- when transferring an employee to another permanent job within the Bank's divisions included in the List of divisions, in the event that the existing knowledge in the field of AML/CFT/FPWMD is not enough to perform the labor function;
- when entrusting an employee of the Bank with work not stipulated by the employment contract concluded with him, when this does not entail changes in the terms of this contract.

The volume, timing and content of the unscheduled (targeted) briefing on AML/CFT/FPWMD are determined by the Bank independently in each specific case.

Training (scheduled briefing) employees of the Bank's divisions included in the List of divisions also undergo in the course of their work. Scheduled briefing is carried out at intervals established by the Bank, subject to the following conditions:

- training of the Responsible employee is carried out at least 2 (two) times a year;
- training of employees of the AML/CFT/FPWMD unit and employees of the Bank's structural units included in the List of units is conducted at least once a year.

The content of the AML/CFT/FPWMD training forms is determined by the Bank based on the position held by the employee, his level of qualification and specific job function.

Documents (or their copies) certifying that the Bank’s employee has completed AML/CFT training and knowledge tests are stored in the Bank during the entire period of his work in electronic form in case of passing a distance learning course on the Portal of the Training Center and (or) in hard copy in employee's personal file.

The AML/CFT/FPWMD knowledge of the Bank's employees is checked on a regular basis, at least once a year. The initial examination of the knowledge of the Bank's employees on AML/CFT/FPWMD is carried out no earlier than ten working days, but no later than two months from the date of the introductory (initial) briefing. Periodic and unscheduled AML/CFT/FPWMD knowledge checks are carried out in the course of work. The form and procedure for checking the knowledge of the

Bank's employees on AML/CFT/FPWMD is determined by the Responsible Officer of the Bank.

10. PROCEDURE FOR PROVIDING INFORMATION AT THE REQUEST OF THE AUTHORIZED BODY

AND information on the transactions of the Clients with cash and other property, on the Beneficial Owners of the Clients, at the request of the Authorized Body, is provided by the Bank on the basis of the current legislation.

The request in the form of an electronic message is sent by the Authorized Body to the Bank by posting it in the Bank's personal account on the website of the Authorized Body on the Internet.

The Bank provides the Authorized Body upon its request with the Bank's information on the transactions of the Clients and Beneficial Owners of the Clients within 5 business days from the date of receipt of the relevant request or the period specified in the request (except for an urgent request).

If the request of the Authorized Body is urgent, the requested information shall be submitted within six hours from the moment of receipt of the request, and if the requested information is stored in the Branch of the Bank - within twelve hours from the moment of receipt of the request.

Responsibility for receiving a request in electronic form, forming a response to a request and timely submission of information to the Authorized Body lies with the department of the FMD.

Employees of the FMD provide information upon request in accordance with the procedure established legislation.

The heads of departments executing the request of the FMD are responsible for the accuracy and relevance and completeness of the information and documents sent to the FMD.

11. FINAL PROVISIONS

This Policy is not exhaustive, all processes are described in detail in the Internal Control Rules for AML/CFT/FPWMD purposes and other internal regulatory documents.

At the request of the correspondent bank of the counterparty, the provisions of this Policy may be disclosed in more detail.