AML and Compliance policy

1. General Provisions

1.1. Terms, Definitions, and Abbreviations

The following main terms, definitions, and abbreviations shall be used for the purposes and in the context hereof:

The Bank means PJSC "SOVCOMBANK", including branches, representative offices, additional offices, credit and cash offices, and cash desks outside the cash operating unit.

The Beneficial Owner means an individual, ultimately, directly or indirectly (through third parties) owns (holds a dominant share exceeding 25 percent of the capital) a corporate Customer, or directly or indirectly controls actions of a Customer. The Beneficial Owner of the individual Customer shall mean this individual unless there are grounds to think that another individual acts as the Beneficial Owner.

The Banking Group means companies under control or significant influence of PJSC "SOVCOMBANK". To determine the list of Group Companies, control and significant influence shall be defined in accordance with International Financial Reporting Standards recognized in the Russian Federation.

The Beneficiary means a person who is not a direct participant in the operation, for the benefit of whom the Customer acts, including on the basis of an agency agreement, a commission and a trust agreement, upon performance of operations with money and other property.

Criminally Obtained Income means money or other property obtained as a result of a committed crime.

Identification means a set of measures to ascertain information on Customers, their Representatives, Beneficiaries and Beneficial Owners as defined by national legislation, to confirm the accuracy of these information using original documents and / or duly certified by the national legislation to confirm the accuracy of this information using original documents and/or duly certified copies.

The Customer means an individual, a self-employed entrepreneur, a person engaged in private practice in accordance with the procedure established by the legislation of the RF, a legal entity (including a credit institution), an unincorporated foreign structure serviced or being accepted for servicing at the Bank as well as persons applying to the Bank to perform onetime operations, including operations without opening a bank account (deposit).

The Shell Company means a legal entity that is created to participate in money laundering schemes, tax evasion, concealment of corruption and other crimes. This legal entity does not carry out real economic activity (generally, the place of registration is offshore jurisdiction or nominal, or trust property, which is regulated by the legislation of this state), or the ultimate beneficial owner is an individual who, due to his financial condition, social status, age, cannot be the owner of the business.

Compliance control – set of measures aimed to identify compliance risks (including regulatory, country and ML/TF risk), as well as to develop measures to prevent and minimize them.

Counterparty – individual or legal entity, including foreign individual or legal entity who is a party in civil law relations with a member of the Banking group

Legalization of Criminally Obtained Income (Money Laundering) means giving a legal form to the possession, use or disposal of funds or other property obtained as a result of a crime.
ML/TF means money (criminally obtained income) laundering or terrorism financing;
AML/CTF means anti-money laundering and combating the terrorism financing.
The Internal Control Rules (ICR) - an internal organizational and administrative document aimed at countering the legalization (laundering) of proceeds from crime, the financing of terrorism and the financing of the proliferation of weapons of mass destruction. It is developed by each member of the Banking Group, taking into account the specifics of their activities and the requirements of the current AML / CFT legislation
Politically Exposed Persons means individuals, who have (or have been previously assigned) important government functions (including duties in a foreign State), for example, Heads of State or government, senior politicians, senior government, judicial officials, senior military officials, senior executives of state owned corporations, and important political party officials.
RF- Russian Federation
The Sanctions Lists mean lists of countries, territories, individuals and legal entities, industries, vessels and types of activities, in respect of which international economic restrictions are applied, drawn up in accordance with the internal documents of the Bank and regulations of the RF, foreign states and international organizations;
Authorized body - a federal executive body that takes measures to counter the legalization (laundering) of proceeds from crime, the financing of terrorism and the financing of the proliferation of weapons of mass destruction.
T**he Banking Group Members**: for the purposes of this Policy, the Banking Group Members shall mean the companies of the Banking Group engaged in financial activities.
The FATF means the Financial Action Task Force on Money Laundering – an intergovernmental body, which set worldwide standards in the field of anti-money laundering and combating the terrorism financing.
Terrorism Financing means providing or raising funds, or provision of financial services while being aware that they are intended for financing a terrorist group (organization), or to support an organized group, an illegal armed group, or a criminal community (criminal organization).
WMD - financing the proliferation of weapons of mass destruction

1.2. Scope of Application

PJSC Sovcombank, being the Parent Credit Organization of the Banking Group of PJSC Sovcombank, in order to exclude the involvement of the Banking Group, its leaders and employees in the legalization (laundering) of proceeds from crime, financing terrorism and financing the proliferation of weapons of mass destruction, approves this Compliance control and Counteracting Legalization (Laundering) of Criminally Obtained Income (Money Laundering),

Terrorism Financing and Financing the proliferation of weapons of mass destruction Policy of PJSC “SOVCOMBANK" (hereinafter referred to as the Policy).

Policy initiating business unit: the Compliance and Fraud Management Department.

1.3. Main Areas, Goals and Objectives of the Policy

The Policy determines general principles and approaches of the Banking Group Members implemented for the purposes of compliance control and AML/CTF/WMD. All Banking Group Members involved in financial transactions are required to apply the provisions of the Policy when organizing internal processes, as well as developing internal regulatory documents.

The main goal of the Policy is to create an efficient compliance control system for AML / CFT / WMD purposes, which minimizes the risks of involving and using employees and services provided by the Banking Group for purposes, as well as its individual participants for ML / CFT / WMD and other illegal actions.

The objectives of this Policy are as follows: - ensuring the functioning of the internal control systems in the Banking Group in accordance with the legislation in the field of AML / CFT and WMD; - compliance with international requirements and agreements on foreign economic policy; - ensuring an effective process of interaction with government agencies, national, foreign and international organizations and institutions on AML / CFT and WMD issues. The Banking Group members organize their work based on the following principles: -creating and maintaining the relevance of internal control systems for AML / CFT and WMD purposes in compliance with the general provisions and principles set out in this Policy; - development of own rules and procedures for compliance control and AML / CFT on the basis of national legislation applicable both to national AML / CFT requirements and to each type of activity of the Banking Group members and their unification with the Banking Group standards; - minimization of risks associated with the involvement in AML / CFT schemes of each of the participants and the Banking Group as a whole; - participation in information exchange for AML / CFT purposes between members of the Banking Group.

When implementing internal control measures for AML / CFT / WMD purposes, the members of the Banking Group are guided by the current legislation of the Russian Federation and this Policy.

2. General Principles

The Banking Group Members shall take necessary measures to prevent operations and/or transactions that are directly or indirectly related to the laundering of criminally obtained income (money), as well as to exclude the possibility of Clients conducting transactions related to the financing of terrorist activities and the proliferation of weapons of mass destruction.

The main goals and principles of functioning of the compliance control system in the field of AML/CTF/WMD are as follows:

- participation of all employees of the Banking Group Members, regardless of their position held and within their official duties, in the events aimed at implementing the Policy and the Internal Control Rules (ICR);
- appointment of responsible employees (RE) or special officials (SO), and, if necessary, the creation of separate units in the organizational structure responsible for implementation, for keeping up-to-date and for ensuring the implementation and control of the Policy principles and the ICR;
- protection of the Banking Group from criminal proceeds; - ensuring that the Banking Group Members comply with the requirements of national and international legislation, international practice, regulations in the field of compliance control and AML/CTF/WMD;
- exclusion of the involvement of the Banking Group, its leaders and employees in the implementation of ML / FT / WMD; - exclusion of the involvement of foreign counterparties, shareholders and partners of the Banking Group members in transactions that violate the laws of foreign states and international organizations, as well as those related to the defense and intelligence sectors of the RF.

The Banking Group Members shall organize the internal control system taking into consideration requirements of national legislation, basic principles, as well as international and Russian recommendations in the field of AML / CFT / WMD, and in accordance with the international standards (to the extent that does not contradict the Russian Federation legislation) including implementation of:

- “Know Your Customer” principle and due diligence;
- Risk-based approach principle;
- Customers' activities monitoring; - Reporting (reports on suspicious operations and transactions);
- Personnel training.

Measures taken to prevent compliance risks and ML/TF risks in relation to Counterparties are similar to the measures applied according to this Policy in relation to Customers.

"Know Your Customer" Principle

“Know Your Customer” principle provides for the identification, examination , analysis and verification of information and documents of Banking Group Members’ Customers, subject to all due diligence measures.

The Banking Group Members identify the Customer both before onboarding and when the Customer perform different types of operations and transactions. Customer identification may not be carried out in the cases established by the current legislation of the Russian Federation, except for cases when there are suspicions that the Client's activity or a separate operation / transaction is related to ML / FT / WMD

The international standards shall mean the FATF recommendations and documents of the Wolfsberg Group that establish principles and standards in the field of AML/CTF (http://www.fatf-gafi.org; http://wolfberg-principles.com).

Establishment and identification of the Beneficial Owners of the Customers is an integral part of the identification procedure. The identification of the Beneficial Owners may not be carried out in cases established by the current legislation of the RF.

The Banking Group Members shall take sufficient and reasonable measures to establish possible actions of the Customer in the interests or to the benefit of third parties, as we as to identify the Beneficiaries, except the cases established by the current legislation.

At the stage of the implementation of “Know Your Customer” principle, the Banking Group Members shall identify politically exposed persons among the individual Customers who are serviced or being accepted for servicing. To determine the status of the Customer as a politically exposed person, the Banking Group Members shall use the classification criteria established by the current legislation of the RF, as well as recommendations of international organizations and foreign competent authorities such as the FATF, the Wolfsberg Group, the US Financial Crimes Enforcement Network (FINCEN), and the European Union. While onboarding a politically exposed person the Banking Group Members shall take reasonable measures to determine the sources of money and pay special attention to the operations of this Customer.

In full compliance with the current legislation and taking into account the needs of the business in achieving financial results, the Banking Group Members shall apply a riskbased approach in implementing the “Know your customer” principle.

The Banking Group Members shall apply an integrated approach to the implementation of the “Know your customer” procedure in relation to each of the potential customers in such a way as to ensure all legislatively established identification procedures. 2.1.8.“Know Your Customer” principle implies not only collection, analysis, processing and recording information about the client, his representative, beneficiary and beneficial owners, but also maintaining the relevance of the information received in the manner and terms established by the current legislation.

Due Diligence

As a part of the implementation of due diligence measures, the Banking Group members, while onboarding, as well as when servicing the Customer, verify the information received from the Customer, including using external sources of legally available information.

The Banking Group Members:

- shall not open and maintain accounts (deposits) for anonymous owners, that is, to the person who opens the account (deposit) without submission of the documents required for Customers' identification, and also shall not open and maintain accounts (deposits) for owners using fictitious names (pseudonyms);
- shall not open accounts (deposits) for individuals without personal attendance of the person opening the account (deposit) or his Representative;
- shall not conclude a bank account (deposit) agreement and shall not provide other banking services to the Shell Companies;
- shall not conclude a bank account (deposit) agreement with the Customer in case the Customer or its Representative does not provide all the documents required for identification;
- shall take all necessary measures to identify persons, in respect of whom there is an information on their possible participation in terrorist or extremist activities, in involvement in the proliferation of weapons of mass destruction among potential 8 clients, clients making one-time transactions, as well as clients who are on a permanent service.

The Banking Group Members have the right to refuse to conclude an agreement or to execute the client's order to perform an operation, with the exception of operations for crediting funds, if there is a suspicion that the operation is being performed or an account is being opened for ML / FT purposes.

Updating Data on the Customer

In order to keep information about Clients up to date, members of the Banking Group on a regular basis and in accordance with national legislation shall update information about the Client, his representative, beneficiary and beneficial owner, that was obtained as a result of identification

Information on the Customer may also be revised and updated if the Customer performs any significant actions (for example, opening a new account) as well as upon receipt of information about changes in the information previously provided by the client.

Risk-Based Approach Principle

To manage the risk of ML/TF, the Banking Group Members shall perform procedures for identification, assessment, monitoring, analysis, control, and minimization of the risk level, and shall take measures to prevent realization of the risk..

The ML/TF risk shall be managed on the basis of a risk-based approach that allows the application of AML/TF measures which are commensurate with the assessed risk. Upon implementation of the risk-based approach, the group members shall evaluate the following types of risks: - the risk of Clients performing operations for ML/TF purposes (hereinafter referred to as the Customer's risk); - the risk of involvement of Banking Group Members and their employees in the use of the services for ML/TF purposes (hereinafter referred to as the Service risk); - the risk of used and planned for use technologies by the Banking Group members (hereinafter - the Risk of technologies for providing services).

The Customer's risk assessment represents the result of the analysis of the documents, details and information about the Customer, its activities and operations performed by the Customer, which are available to the Banking Group Members. The Customer's risk Assessment shall apply to all the Customers, including the Customers performing onetime transactions.

The Customer's risk shall be assessed on a three-level scale (Low, Medium, High) for the aggregate of the following categories of risk categories: - the risk on a Customer and/or beneficial owner type; - the country risk; - the risk connected with a type of the transaction performed by the Customer.

The principle of the risk-based approach consists in the differentiated application of the “Know your Customer” principle, depending on the level of risk assigned to the Customer. If the Customer, its activities or transactions carried out by him bear an increased risk of ML / TF or country risk, then such Customer should be subject to enhanced due diligence measures while implementing the “Know Your Customer” principle. The members of the Banking Group independently determine in their internal regulations the content and nature 9 of measures taken depending on the level of risk of the Customer, taking into account the requirements and recommendations of the current legislation of the RF.

The Banking Group Members take legal and available measures being available in the circumstances concerned to assess, control and reduce the ML / TF Risk in the Banking Group. Herewith, the following factors are considered:

- availability of procedures enabling to record Customer’s data changes revealed in the process of Customer’s maintenance;
- analysis of the ways of using certain products for laundering the proceeds of crime, financing terrorism and financing the proliferation of weapons of mass destruction and transformation of these methods;

- analysis of training procedures and analysis of the degree to which employees understand their tasks and actions in the field of AML / CFT / WMD;
- efficiency of interaction between the RE, SO, the subdivision responsible for internal control for AML / CFT purposes and other subdivisions at the level of the internal corporate structure of the Banking Group members, both individual organizations, and between members of the Banking Group as legal entities

The country risk arises if a Banking Group Member has information that the Customer, the Beneficial Owner of the Customer, the Customer's counterparty, or the Customer counterparty's bank is registered in a foreign country (territory), indicating that:

- the country (territory) is included in the list of countries that do not comply with the recommendations of the Financial Action Task Force on Money Laundering (FATF);
- the country (territory) is subject to international sanctions approved by the RF (for example, measures taken by the RF in accordance with United Nations Security Council's resolutions);
- the country (territory) is subject to special economic measures in accordance with Russian legislation;
- the country (territory) is identified by international organizations, including international non-governmental organizations, as providing finance or support for terrorist activities;
- narcotic drugs are illegally manufactured or shipped in the country (territory);
- the country (territory) allows free drug traffic (except for the countries (territories) that use narcotic drugs for medical purposes only);
- the country (territory) is classified by international organizations, including international non-governmental organizations, as having heightened level of corruption and/or other criminal activity;
- the country (territory) provides a preferential tax treatment and/or does not provide for disclosure and information provision upon financial transactions settlements (offshore territories); and if there is information that the Customer, the Beneficial Owner of the Customer, the Customer's counterparty, the country (territory) of registration of any of the operation/transaction's party and/or the Customer counterparty's bank, is subject to international economic restrictions

The information contained in international sanctions lists is also used to assess the level of country risk, an ongoing operation or transaction. The relevance of such information is established on a daily basis. The processes and methods of maintaining the information relevance are determined independently by each Banking Group member, taking into account the available information, financial and work resources.

The Banking Group Members shall take all necessary measures to protect foreign Counterparties, shareholders and partners from involvement in conducting transactions with heightened country risk.

The Banking Group Members:
- shall define a set of criteria used for risk assessment in the internal regulations;
- shall review and update risk management procedures on a regular basis.

Customer's Activities monitoring

In addition to Customers due diligence measures implementation, the Banking Group Members consider their Customer's activities on a regular basis and monitor their operations using automatic means and programs.

The system automatically generates an online alert about an operation that requires consideration and decision making on it by a compliance unit employee; such operation shall not be performed until a relevant decision is made.

When establishing Customer's activities monitoring procedures, the Banking Group Members shall consider frequency, volume, and nature of the Customers' operations, the Customer's risk level and the risk of used products/services. The regularity and depth of monitoring shall be determined in accordance with the current legislation and in line with the risk-based approach.

The result of the Customer's operations analysis is a significant factor for making a decision on an enhanced study of the Customers' activities (monitoring of the activities). The Customer's activities shall be monitored:
- on real time basis upon performing of operations;
- during the subsequent monitoring of operations/activities of the Customers.

Monitoring procedures include analysis of Customer's operations and of its activities and comparison of the obtained data with information on the activity being typical for such Customer

The Banking Group Members shall suspend operations with money or other property in accordance with the terms and conditions, and procedures determined by the current legislation of RF.

Banking Group Members, carrying out transactions with funds and other property have the right to refuse to execute the Client's order to perform an operation, except for operations for crediting funds received to the Client's account, for which the documents required to record information in accordance with the provisions of the current legislation of RF have not been submitted , as well as if a member of the Banking Group has suspicions that the operation is being performed for ML / FT purposes.

Correspondent Banking Services (applicable only to members of the Banking Group - credit institutions).

The Banking Group Members shall not open “payable through” accounts since it is impossible to reliably identify actual users of these accounts.

The Banking Group Members shall apply a conservative approach to establishing correspondent relations. A correspondent shall comply with the requirements of the legislation of RF and internal policies of the Banking Group. The Banking Group Members shall not establish and maintain relations with non-resident banks that do not have permanent management bodies in the territories of countries, in which they are registered.

Prior to opening of an account and upon annual updates of the respondent's dossier, the Banking Group members study the activities of the respondent bank, including the nature of the business and transactions, the volume of transactions, the main counterparties in order to make sure that the client meets the Bank's compliance and AML / CFT requirements

Reports on Suspicious Operations and Transactions

Upon detection of operations (transactions) with money or other property of the Customer that meet statutory criteria, or operations (transactions) that may be associated with ML/TF, the Banking Group Members shall inform the Authorized Body in the manner established by the legislation.

Upon development of reporting procedures, the Banking Group Members shall consider the following aspects:

- all employees of a Member of the Banking Group are involved in the collection of information on operations, which are to be reported to the Authorized Body;
- reports are submitted to the Authorized Body within timeframes determined by the national legislation or as soon as possible unless otherwise specified by the Russian legislation;.

- all actions taken in relation with operations, which are to be reported to the Authorized Body, are documented and retained in accordance with internal regulations;
- details of operations, which are to be reported to the Authorized Body, and any contacts with the Authorized Body or other public authorities in relation to these operations are documented;
- reports on operations sent to the Authorized Body shall contain information on the Customer, operation or activity to the extent provided for by the Russian legislation.

Training of Personnel of the Banking Group Members

High-quality personnel training on AML/CTF issues shall be one of the main tools used to create an efficient AML/CTF internal control system.

The Banking Group Members shall determine the structural divisions whose employees must undergo training on AML /CFT /WMD, taking into account the requirements of national legislation, functional responsibilities of employees and features of the functioning of the internal control system for AML /CFT /WMD of the Banking groups.

The Banking Group Members shall conduct personnel training on a regular basis.

For RE/SO, professional development is required at least once a year.

Training of employees is carried out upon approval and / or entry into force of new legislative normative acts in the field of AML / CFT, when changing internal regulatory and administrative local documents, as well as in order to increase the level of knowledge. Training is conducted by RE / SO appointed by each participant of the Banking groups. The frequency and timing of such training are established in accordance with the requirements of the current AML / CFT legislation, taking into account the specifics and direction of activities of a member of the Banking Group.

The need to conduct training on AML / CFT issues also arises when employees are transferred to another position subject to a significant change in their job responsibilities.

3. Record keeping

The Banking Group Members shall keep documents and information obtained upon implementation of the ICR, including documents and/or information obtained upon Customer identification; accounting records and information on performed operations as 12 well as documents concerned to relations with the Customers and other persons cooperating with the Banking Group Members, in electronic form and/or in hard copy.

The Banking Group Members shall keep the specified documents and information obtained upon Customer identification for at least five years since the date relationships with the Customer have been terminated

4. Confidentiality of information

Employees of the Banking Group Members who, by virtue of their official duties, have access to confidential information shall comply with the requirements on its non-disclosure to third parties.

Employees, when preparing documents containing confidential information, including internal official correspondence, take reasonable and sufficient measures to ensure the confidentiality of information in accordance with the procedures adopted by the Banking Group members in the field of compliance with information security requirements, as well as requirements for non-disclosure of applied measures in order to AML / CFT / WMD.

The Members shall exchange information within the Banking Group for the purposes of AML/CTF/WMD in line with the applicable legislation of RF.

5. Control

The activities of the Banking Group Members acting as the credit institutions shall be controlled by the Central Bank of the Russian Federation (the CB of the RF, www.cbr.ru), the activities of other Banking Group Members shall be controlled by the relevant authorities that are responsible for compliance with the requirements of the legislation of the RF.

To comply with the Policy the Banking Group Members shall perform internal and external audits on a regular basis, but at least once a year

2021