APPROVED
By the Supervisory Board decision
of PJSC "Sovcombank"
(Protocol No.16 dd. September 13, 2019)

COMPLIANCE CONTROL AND COUNTERACTING THE LEGALIZATION OF CRIMINALLY OBTAINED INCOME (MONEY LAUNDERING) AND TERRORISM FINANCING POLICY OF THE PJSC "SOVCOMBANK" BANKING GROUP

Kostroma, 2019

Table of Contents

1. GENERAL PROVISIONS

1.1. Scope of Application

1.1.1. In order to prevent involvement of the Banking Group, its management, and employees in the legalization (money laundering) of Criminally Obtained Income and Terrorism Financing, PJSC “SOVCOMBANK”, being a Parent Credit Institution of PJSC “SOVCOMBANK” Banking Group, approves this Compliance control and Counteracting Legalization (Laundering) of Criminally Obtained Income (Money Laundering) and Terrorism Financing Policy of PJSC “SOVCOMBANK" (hereinafter referred to as the Policy).

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

1.2. 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, including legal entities, several legal entities, or a group of related legal entities), owns (holds a dominant share exceeding certain percentage of the capital) a corporate Customer, or directly or indirectly controls actions of a corporate or an individual Customer, including an opportunity to determine decisions adopted by the 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 party to an operation, to the benefit of whom the Customer acts, including on the basis of an agency agreement, a commission agreement, 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 establish information on the Customers, their Representatives, Beneficiaries, and Beneficial Owners defined 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 Russian Federation, 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 not physically present in the jurisdiction, in which it has been incorporated.
- **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 making ownership, use, or disposal of money or other property obtained as a result of the committed crime appear to be lawful.
- **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)** means the Internal Control Rules of PJSC "SOVCOMBANK" to counteract the legalization of criminally obtained income (money laundering) and terrorism financing.
- **Politically Exposed Persons** means individuals, who are or have been entrusted with a prominent public function (including duties in a foreign State), for example Heads of State or of government, senior politicians, senior government, judicial officials, senior military officials, senior executives of state owned corporations, and important political party officials.
- **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 imposed in accordance with the internal documents of the Bank and regulations of the Russian Federation, foreign States, and international organizations, are applied;
- **The Authorized Body** means a federal executive body taking measures to counteract the legalization of criminally obtained income (money laundering) and terrorism financing and proliferation of weapons of mass destruction financing.
- **The 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 inter-governmental 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).

1.3. Main Areas, Goals and Objectives of the Policy

1.3.1. The Policy determines general principles and approaches of the Banking Group Members implemented for the purposes of compliance control and AML/CTF. The Banking Group Members shall apply the provisions of the Policy while organizing internal processes and drafting internal regulations.

1.3.2. The main goal of the Policy is to create an efficient compliance control and AML/CTF system, which minimizes the risks of using the Banking Group and the services it provides for the purposes of ML/TF.

1.3.3. The objectives of this Policy are as follows:

- to ensure functioning of internal control systems of the Banking Group for the purposes of AML/CTF in accordance with the provisions of the legislation;
- to regulate the operational coordination principles of compliance control and AML/CTF activities of the Banking Group Members;
- to ensure an efficient process of interaction with public authorities, national, foreign and international organizations and institutions on AML/CTF issues.

1.3.4. To join efforts in preventing involvement in performance of operations related to ML/TF, the Banking Group Members shall organize their work on the basis of the following principles:

- development, implementation and improvement of internal controls for the AML/CTF purposes are based on general principles and guidelines outlined in the Policy;

- development of own rules and procedures for the purposes of compliance control and AML/CTF on the basis of the national legislation and their unification with the standards of the Banking Group;
- minimization of risks associated with involvement into the ML/TF schemes within each of the Banking Group Members as a whole;
- exchange of information between the Banking Group Members for the AML/CTF purposes.

1.3.5. By implementation of internal control measures for the purposes of AML/CTF, the Banking Group Members shall be governed by the Russian Federation applicable legislation 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 criminally obtained income (money) laundering as well as to exclude the possibility of conducting operations related to the terrorist activities financing by the Customers.

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

- participation of all employees of the Banking Group Members, regardless of their position, within their official duties, in events aimed at implementing the Policy and the ICR;
- presence of dedicated units that support, implement, provide implementation and tools for implementing the Policy 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;
- protection of the Banking Group, its management and employees from involvement in implementation of ML/TF;
- protection of foreign counterparties, shareholders and partners of the Banking Group Members from involvement in implementation of operations that violate the laws of foreign states and international organizations, as well as those related to the defense and intelligence sectors of the Russian Federation.

The Banking Group Members shall organize the internal control system taking into consideration the basic principles and recommendations in the field of AML/CTF, and in accordance with the international standards (to the extent that does not contradict the Russian Federation legislation) including implementation of:[1]

- "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.

2.1. "Know Your Customer" Principle

2.1.1. "Know Your Customer" principle provides for identification, study, analysis, and verification of reliability of information and documents in respect of all Customers the Banking Group Members taking into account compliance with due diligence.

2.1.2. The Banking Group Members identify the Customer both before onboarding, as well as when the Customer perform different types of operations and transactions. The Customer may not be identified in cases established by the current legislation, except the cases when there are suspicions that the Customer's activity or any single operation/transaction is related to ML/TF.

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

2.1.4. The Banking Group Members shall take all applicable and reasonable measures to establish the possible fact that the Customer acts in the interests or to the benefit of third

[1] 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).

parties as well as to identify the Beneficiaries, except the cases established by the current legislation.

2.1.5. At the stage of 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 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.

2.1.6. In the light of business's needs and in full accordance with the current legislation, the Banking Group Members shall apply a risk-based approach of "Know Your Customer" principle implementation.

2.1.7. The Banking Group Members shall comprehensively implement "Know Your Customer" procedures for each of the potential Customers in such a way as to ensure that the procedures for identification and its results documenting are performed.

2.1.8. "Know Your Customer" principle implies not only collection, analysis, and processing of information on the Customer, its Representative, Beneficiary, and Beneficial Owners, but also updating the obtained information, therefore, the Banking Group Members shall provide regular updates of previously obtained information on the specified persons.

2.1.9. Due Diligence

2.1.9.1. As a part of implementation of due diligence while onboarding as well as the service providing to the Customer, the Banking Group Members shall verify information received from the Customer, including using external sources of legally available information.

2.1.9.2. The Banking Group Members:

- shall not open and shall not 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 shall not 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, among potential Customers as well as the Customers being serviced.

2.1.9.3. The Banking Group Members may repudiate to conclude bank account agreement if there are any suspicions that the account is being opened for the purposes of ML/TF.

2.1.10. Updating Data on the Customer

2.1.10.1. In order to keep the information of the Customers in relevant status, the Banking Group Members shall update information of the Customer, its Representative,

Beneficiary, and Beneficial Owner obtained as a result of identification on a regular basis in accordance with the national legislation.

2.1.10.2. 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 revealing the changes in the Customer's management bodies, the changes in ownership structure, the risk level assigned to the Customer, etc.

2.2. Risk-Based Approach Principle

2.2.1. 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 take measures to prevent realization of the risk.

2.2.2. The risk of ML/TF shall be managed on the basis of a risk-based approach that makes it possible to apply AML/CTF measures being proportionate to the assessed risk.

Upon implementation of the risk-based approach, the group members shall evaluate the following types of risks:

- the risk of conducting the operations in the purposes of ML/TF by the Customer (hereinafter referred to as the Customer's risk);
- the risk of involvement into the use of the services for the purpose of ML/TF by the Banking Group Members and their employees (hereinafter referred to as the product risk).

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

2.2.4. The Customer's risk shall be assessed pursuant to a three-level scale (Low, Medium, High) for the complex of the following categories of risks:

- 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.

2.2.5. The risk-based approach principle involves a differentiated operation of "Know Your Customer" principle depending on the risk level assigned to the Customer. If the Customer, its activity or operations carry a heightened ML/TF or country risk, enhanced due diligence measures shall be applied to such Customer upon of "Know Your Customer" principle implementation. The Banking Group Members shall independently determine content and nature of measures taken depending on the Customer's risk level in the internal regulations in line with the requirements and recommendations of the current legislation.

2.2.6. The Banking Group Members take legal measures being available in the circumstances concerned to assess, control, and reduce the overall ML/TF and country risk level 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;
- analysing methods of certain products use for laundering proceeds of crime and terrorism financing, and transformations of these methods;
- training procedures analysis and the degree of understanding by the employees of their tasks and actions in the AML/CTF area;
- efficiency of interaction between the business unit responsible for AML/CTF internal control and other business units of the Bank.

2.2.7.1. 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 Russian Federation (for example, measures taken by the Russian Federation 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.

2.2.7.2. The Banking Group Members shall automatically monitor international sanction lists on a daily basis to assess the country risk level of the Customer or the Customer's activity (operation) using both internal software developments and purchased software products.

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

2.2.8. The Banking Group Members:

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

2.3. Customer's Activities monitoring

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

2.3.2. 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.

2.3.3. 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 of the Banking Group. The regularity and depth of monitoring shall be determined in accordance with the current legislation and in line with the risk-based approach.

2.3.4. 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.

2.3.5. Monitoring procedures include Customer's operations analysis, its activities and comparison of the obtained data with information on the activity being typical for the customer and/or areas of activities.

2.3.6. 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.

2.3.7. Except for the credit of funds transferred to the Customer's account the Banking Group Members are entitled to refuse to process the Customer's transaction orders, if the documents required for information recording in accordance with the provisions of the current legislation have not been submitted as well as if a Member of the Banking Group has suspicions that the operation is being performed for the purposes of ML/TF.

2.3.8. The Banking Group Members is entitled to terminate the bank account (deposit) agreement with the Customer in cases provided for by the current legislation.

2.3.9. **Correspondent Banking Services**

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

2.3.9.2. The Banking Group Members shall apply a conservative approach to establishing correspondent relations. A correspondent shall comply with the requirements of the legislation 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.

2.3.9.3. Prior to opening of an account and upon annual updates of the dossier the Banking Group Members shall consider the activities of the correspondent bank, including the nature of the business and transactions, volume of the transaction, and major counterparties in order to make sure that the customer meets the requirements of the Bank in the field of compliance and AML/CTF.

2.4. Reports on Suspicious Operations and Transactions

2.4.1. 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.

2.4.2. 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 collection of information on operations, which are to be reported to the Authorized Body;
- reports are submitted to the Authorized Body within time limits specified 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 the 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.

2.5. Training of Personnel of the Banking Group Members

2.5.1. 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.

2.5.2. The Banking Group Members shall determine the employees who should undergo training on AML/CTF considering the requirements of the national legislation as well as on the basis of the functional responsibilities of the employees and considering the peculiarities of the AML/CTF internal control system.

2.5.3. The Banking Group Members shall conduct personnel training on a regular basis, but at least once a year. If needed, additional personnel training is conducted with regard to approval and enforcement of new legislative and regulatory requirements in the field of AML/CTF as well as to improve the personnel's knowledge.

2.5.4. Upon transferring into another job position or upon change in job responsibilities employees are obliged to retake AML/CTF training.

3. RECORD KEEPING

3.1. 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 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.

3.2. The Banking Group Members shall retain documents and/or information obtained upon Customer identification for at least five years since the date relationships with the Customer have been terminated.

4. CONFIDENTIALITY OF INFORMATION

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

4.2. Comply with the policies regulating handling of confidential information, including internal official correspondence; employees shall take adequate and sufficient measures to ensure confidentiality of information in accordance with the procedures adopted by the Banking Group Members regarding compliance with information security requirements and requirements to nondisclosure of applicable AML/CTF measures.

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

5. CONTROL

5.1. 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) and the Federal Financial Monitoring Service (www.fedsfm.ru).

5.2. 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.