Joint Stock Company Commercial Bank "PrivatBank"

APPROVED
Decision of the Supervisory Board
Minutes No.53/20
dated September 29, 2020

Policy
of Prevention and Counteraction to Legalization (Laundering) of Proceeds from Crime, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction

Registration number: 2020/7038894
Document status: Open
Approval data:
decision of the Supervisory Board, Minutes No.24/19 dated November 21, 2019;
decision of the Management Board, Minutes No.20 dated May 22, 2018.

Kyiv

Policy of Prevention and Counteraction to Legalization (Laundering) of Proceeds from Crime, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction

Contents

1. General Provisions

1.1 The Policy of Prevention and Counteraction to Legalization (Laundering) of Proceeds from Crime, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction (hereinafter - the AML/CFT Policy) is applicable to structural units of JSC CB PrivatBank (hereinafter - the Bank), including all its standalone units and those located in other jurisdictions, to employees, business partners of the Bank, participants of groups / payment systems of which the Bank is a member, or who are participants of organizations / payment systems established by the Bank, clients enabling financial operations with the Bank's support on the territory Ukraine and abroad in accordance with international treaties of Ukraine, the binding nature of which has been approved by the Verkhovna Rada of Ukraine and/or clients' counterparties.

1.2 A core objective of the AML/CFT Policy is to determine and approve general principles of the Bank's compliance with the Ukrainian legislation on AML/CFT issues, to prevent using the Bank's services for legalizing (laundering) proceeds from crime, financing terrorism and financing the proliferation of weapons of mass destruction (hereinafter - ML/FT) and counteract to any other activities preceding or facilitating ML/FT.

1.3 The AML/CFT Policy describes the basic rules and standards of the Bank all employees are obliged to comply with in order to ensure steadfast implementation of the AML/CFT laws of Ukraine (hereinafter - Local AML/CFT Laws) and international requirements and standards.

1.4 The following AML/CFT rules and standards of the Bank are defined:

1.4.1 Conscientious compliance with all AML/CFT specific requirements, rules and procedures prescribed by the Local AML/CFT Laws, international banking standards and internal documents of the Bank.

1.4.2 Strict compliance with the requirements and restrictions, as well as prohibitions related to AML/CFT set forth in local and international requirements.

1.4.3 Zero tolerance for any manifestations of illegal or criminal activities of persons with whom the institution enters into business (contractual) relationships and / or to whom it provides banking or other services.

1.4.4 Continuous use of all possible means, methods and techniques to avoid being involved in suspicious or illegal business (money laundering, fraud, activities of terrorist organizations and groups operating or collecting money in the country, cross-border transit of criminal or illegal assets through the country, etc.).

1.4.5 Giving priority to customer proper or enhanced due diligence (hereinafter - CDD/EDD) consistent with the level of risks determined/identified over profit-making or obtaining benefits from customer acquisition or servicing. Understanding that customer due diligence measures is prerequisite for the Bank to provide the highest

quality services.

1.4.6 Commitment to high AML/CFT standards, forming best banking practices when applying preventive control methods, identification and implementation of advanced AML/CFT models and technologies.

1.4.7 Unconditional cooperation with the government and other authorities, organizations and institutions, including financial and lending entities, in their AML/CFT activities.

1.5 The main AML/CFT priorities and tasks of the Bank include:

1.5.1 Protecting the legitimate interests of citizens, the society and the State against damage which may be caused by criminal actions in the area of AML/CFT. Protecting the Bank employees from threats and other negative or discriminatory actions related to compliance with the AML/CFT legislation requirements.

1.5.2 Taking all reasonable efforts to prevent any connections (including indirect ones) with ML/FT or fraud.

1.5.3 Careful adherence to AML/CFT rules and instructions developed in order to comply with the Ukrainian legislation requirements, protect the Bank's image, reputation and keep the trust of customers.

1.5.4 Awareness that any violation of laws, internal regulations and procedures, especially in the AML/CFT area, cannot be justified by profit-making. All products shall be developed and implemented, and all business processes shall be maintained strictly in compliance with the Local AML/CFT Laws. Any activities contradicting the Local AML/CFT Laws, internal Bank regulations and this Policy are unacceptable for the Bank, regardless of similar practice being allowed by other market participants or other financial institutions.

1.5.5 Understanding the inevitability of punishment for violating the Local AML/CFT Laws. Money laundering (ML/FT) is a process in which a financial institution is used as a tool to legalize criminal proceeds. Such actions put the institution in potential danger, threaten its reputation and may entail enforcement actions (sanctions) on the part of state financial monitoring entities.

1.5.6 Measurement of the Bank's performance by evaluating the degree to which the institution mitigates risks and threats of being used for AML/CFT. The Bank believes that prevention of such actions is the most efficient mean to prevent money laundering and terrorism financing.

1.6 One of the most important areas of the Bank's relations with external organizations are relations with the state financial monitoring entities, including the body performing the functions of state regulation and supervision over the banks (hereinafter - the National Bank of Ukraine / NBU), Financial Intelligence Unit (hereinafter - FIU) and the central executive authority in charge of formulating and

enforcing the State's AML/CFT policy (hereinafter - the Ministry of Finance of Ukraine).

In order to determine (identify) ML/FT risks (threats), the Bank participates (if necessary) in the national risk evaluation actions undertaken by state financial monitoring entities, authorized government authorities to prevent and/or mitigate negative risk impact.

1.7 Abbreviations used herein:

responsible employee means an employee responsible for financial monitoring in the Bank;

ML/FT means legalization (laundering) of proceeds from crime, financing of terrorism and financing of proliferation of weapons of mass destruction;

UBO means ultimate beneficial owner;

AML/CFT means counteraction to legalization (laundering) of proceeds from crime, financing of terrorism and financing of proliferation of weapons of mass destruction;

List of Terrorists means a list of persons connected with terrorist activities or persons subject to international sanctions, which is formed in accordance with the procedure established by the Cabinet of Ministers of Ukraine;

FIU (Financial Intelligence Unit) means central executive body implementing the state policy of Ukraine in the area of AML/CFT / specially authorized body / State Financial Monitoring Service of Ukraine;

CDD (Customer Due Diligence) means proper due diligence and monitoring measures regarding business relationships and financial operations of persons with whom the institution enters into business (contractual) relationships and / or to whom it provides banking services;

EDD (Enhanced Due Diligence) means enhanced risk oriented due diligence measures regarding the customers the business relationships with whom (financial operations without establishing business relationships) pose a high risk, are proportional to the identified risks and aimed at mitigating them, including by increasing the frequency and scope of business relationship monitoring activities and collection of additional information on business relationships;

SDD (Simple Due Diligence) means simplified risk oriented due diligence measures regarding the customers the business relationships with whom (financial operations without establishing business relationships) pose a low risk, are proportional to the identified risks and may include, in particular, decrease in frequency and scope of business relationship monitoring activities and collection of additional information on business relationships;

PEPs mean politically exposed persons;

SDN (Specially Designated Nationals and Blocked Persons List) means a list of specially designated individuals who are subject to personalized sanctions, compiled and maintained by the Office of Foreign Assets Control (OFAC) of the U.S. Treasury Department;

SSI (Sectoral Sanctions Identifications) means a list of certain activities of individuals who are subject to a ban on funding, participation, and any other actions, which are or may be related to sectoral sanctions applied to specific activities and/or economies of the respective countries.

2. Organization of the Intrabank AML/CFT System and Internal Control

2.1 Organization of the intrabank AML/CFT system provides for:

2.1.1 Creation of an appropriate organizational structure which is shown as three lines of defense in the area of AML/CFT (hereinafter - protection):

The First Line of Defense, which includes: the Bank's business and support units, which directly initiate, implement (provide, support) protection measures, take AML/CFT risks in the course of their activities and are responsible for these risks current management, implement control over protection system functioning;

The Second Line of Defense, which includes: a separate AML/CFT structural unit subordinated to a responsible employee, and the Compliance Division. These structural units make the Bank's managers confident that the protection measures implemented by the 1st and 2nd lines ensure compliance with all requirements and proper functioning;

The Third Line of Defense, which includes: the Bank's Internal Audit Division which carries out an independent assessment of the 1st and 2nd lines effectiveness and an overall assessment of the AML/CFT risk management system effectiveness.

2.1.2 Definitions in the interbank documents, namely:

- the order of vertical interaction between structural units of the lines of defense;
- the order of horizontal interaction within one structural unit of the line of defense and / or between several units of the same line of defense using the principles of functional (permanent), periodic and double control conducted by two (or more) employees ("two pairs of eyes" principle);
- powers of authority, subordination, accountability, availability of processes descriptions and allocation of functional duties, responsibility for their non-performance and / or inaction.

2.2 In order to properly organize and operate the intrabank AML/CFT system (including risk management systems), the Bank shall:

221 Appoint a responsible employee at the level of the Bank's management in accordance with the Ukrainian AML/CFT legislation requirements, with ensuring verification of qualification and impeccable business reputation requirements determined by the NBU regulations. A responsible employee shall be directly accountable to the Bank's Supervisory Board, as well as shall report to it on defense activities. A responsible employee candidacy shall be concurred with the NBU in the order prescribed by the AML/CFT Regulation.

222 Create a separate AML/CFT structural unit directly reporting to a responsible employee of the Bank. Allocate sufficient resources for the functioning of the intrabank AML/CFT system (including a separate AML/CFT structural unit), involve in AML/CFT experienced and trusted staff checked for professional aptitude, impeccable business reputation and trustworthiness when being hired.

223 Ensure permanent functioning of the collegial body to consider problematic and challenging issues associated with the intrabank AML/CFT system - the Compliance and Financial Security Committee.

224 Ensure functioning of an appropriate ML/FT risk management system using a risk-based approach (hereinafter - RBA), which is proportional to the nature and range of the Bank's activities, is uninterruptedly applied and ensures detection, identification, and assessment of all existing and potential ML/FT risks inherent in the Bank's activities (the Bank's risk profile) and its clients (clients risk profile), as well as provides for timely development of measures to manage the ML/FT risks, and mitigate them.

225 Develop and approve the Bank's internal AML/CFT documents to the extent necessary for effective functioning of the intrabank AML/CFT system and the Bank's employees understanding their job duties and powers in the area of AML/CFT.

226 Ensure sufficient information for the Bank's top management, enhance their awareness on issues specified by the AML/CFT Regulation, including ML/FT risks inherent to the Bank's risk profile, as well as informing them about AML/CFT compliance events facilitating the understanding of the consequences which the Bank faces in case of non-compliance with the Ukrainian AML/CFT legislation and actions to manage such risks.

227 Allocate AML/CFT functions between three lines of defense, enhance proper awareness of the Bank's staff, including business units' employees, ensure their fulfillment of the AML/CFT functions (responsibilities) defined by job descriptions, as well as their understanding of responsibility for failure to fulfill job duties and / or inaction.

228 Introduce and constantly improve internal control related to AML/CFT issues, in particular ensure internal audits of the Bank's activities, performed by:

- Compliance Division on initiative of the responsible employee,

- structural units of the Bank and their employees to comply with the requirements of internal AML/CFT documents;

- Internal Audit Division regarding the Bank's compliance with the requirements of the AML/CFT laws of Ukraine, including the adequacy of the measures taken to ensure functioning of an appropriate AML/CFT risk management system.

2.2.9 Investigate new products/services, including new sales channels, use or development of new technologies for existing or new products to properly assess their inherent ML/FT risks and to adequately control them for existing products/services.

2.2.10 Provide regular trainings for the Bank's employees and agents (their employees) to enable them to understand their responsibilities and procedures.

2.2.11 Create and ensure functioning of an effective and timely system for escalating suspicions and problematic AML/CFT issues and procedures for their consideration, including reporting of information/facts regarding violations or possible violations of the AML/CFT laws, as prescribed by the Bank's internal documents.

2.2.12 Introduce an automation system that ensures timely and full performance of responsibilities by the Bank as the primary financial monitoring entity (in particular: detection of threshold and suspicious financial operations, freezing of assets related to terrorism and/or its financing / proliferation of weapons of mass destruction and/or its financing, rejection of operations by persons from the List of Terrorists, rejection of transfers in the absence of payer's (transfer initiator's) and/or recipient's data, provided by the AML/CFT Laws, etc.).

2.2.13 Provide timely detection of threshold and suspicious financial operations (activities), proper information sharing with the FIU, including informing the relevant authorities on freezing/thawing of assets of persons included in the List of Terrorists, and on identified discrepancies in UBO.

2.2.14 Ensure functioning of a proper system for detecting PEPs, taking additional measures regarding them according to the Ukrainian AML/CFT legislation, organize measures to provide the "transparency" of the clients' ownership structures and identify UBOs of clients - legal entities.

2.2.15 Develop and implement CDD/EDD/SDD measures to understand the nature of clients' activities, objectives and expected nature of business relationships with them, which enables the Bank to make sure that the clients' financial operations are compliant with the Bank's existing information about them, their businesses, risk profiles, including, if necessary, the sources of funds/assets origin, detection of UBOs to promptly identify unusual behavior and suspicious financial operations (activities).

2.2.16 In response to requests from the state financial monitoring services, provide necessary documents / information / explanations / arguments, duly confirming the Bank's compliance with the Ukrainian AML/CFT legislation requirements.

2.2.17 Document the actions of the Bank's employees and record events related to the performance of the Bank's AML/CFT obligations.

2.2.18 Keep all documents, data, information (including relevant reports, orders, files) related to the performance of the Bank's AML/CFT obligations within time limits specified by the legislation of Ukraine.

2.2.19 Take other measures to continuously improve the internal AML/CFT system.

2.4 The Bank shall provide a comprehensive, efficient and adequate internal AML/CFT control system in compliance with the principles set out in the NBU Regulation On the Organization of Internal Control Systems in the Banks.

Internal control measures shall ensure compliance with the requirements of this Policy and the AML/CFT laws.

2.5 The Bank identified five components of the internal AML/CFT control system (hereinafter - the components) operating in the Bank at all organizational levels in a mutually integrated manner involving the use of the result of any component while performing other control measures.

I AML / CFT control environment. This component shall include:

- intrabank AML/CFT system organization and functioning;
- allocation of the AML/CFT functions (duties) between three lines of defense;
- level of the AML/CFT culture, participation of all bank employees, including business units' staff, in the AML/ CFT defense system;
- involvement of the Bank's top managers in the AML/CFT risk management;
- organization of staff training, knowledge assessment through testing (certification).

II AML/CFT risk management. This component shall include:

- timely identification, assessment, monitoring, control, mitigation and reporting on ML/FT risks;
- development of methods, tools and models (including scoring) to identify ML/FT risks using a risk-oriented approach;
- implementation of a comprehensive two-phase assessment/reassessment of the Bank's ML/FT risks (the Bank's risk profile), risk of business relationships (financial operations without establishing business relationships) with clients (clients' risk profile);
- ensuring monitoring, control and prevention of violations of ML/FT risk appetite indicators;

– documenting the ML/FT risks results.

III AML/CFT control activities / control procedures. This component shall include:

– description of the AML/CFT processes and control procedures;

– consistent combination of preliminary, current (real-time) and subsequent controls to increase the effectiveness and efficiency of AML/CFT defense measures;

– preventive control methods aimed at preventing AML/CFT violations and risks;

– automated AML/CFT control procedures, the ratio of manual and control procedures, the use of dual control functions;

– documenting all actions of the Bank's employees and recording events related to the Bank's AML/CFT tasks implementation;

– ensuring constant control of subordinate employees by functional and linear managers;

– ensuring periodic control through assessing the effectiveness of AML/CFT control procedures, identifying the features and possibilities of using the Bank's AML/CFT products/services by the Compliance Division.

IV AML/CFT information flows and communications control. This component shall include:

– availability of a system for escalation of AML/CFT suspicions and problematic issues, timely and effective procedure for their consideration, including notification of information/facts regarding cases of violation or possible violation of the AML/CFT laws of Ukraine;

– prompt response to received notifications of violations of the AML/CFT legislation requirements, including those received anonymously, with guarantees of protection and confidentiality;

– ensuring the secrecy of financial monitoring, as well as other confidential AML/CFT information.

V Monitoring the effectiveness of the Bank's internal AML/CFT control system. This component shall include:

– monitoring the effectiveness of the internal AML/CFT control system, reporting (informing) on violations at all organizational levels;

– making timely and appropriate management decisions to improve the efficiency of the internal AML/CFT control system;

- identification of problems and deficiencies in the intrabank AML/CFT system by compliance and internal audit units through inspections of activities (processes, procedures) and informing the Bank's top management on the results of such inspections;

- other measures to improve the internal AML/CFT control system.

3. The Bank's AML/CFT Risk Appetite

3.1 The Supervisory Board of the Bank shall determine the AML/CFT risk appetite (hereinafter - risk appetite) and communicate it to the Bank's Management Board and the responsible employee.

3.2 Risk appetite indicators that determine the amount of AML/CFT risk acceptable for the Bank and the risks that the Bank may accept since the adoption of measures to manage such risks (mitigate them) shall be recorded in the Bank's Risk Appetite Statement.

The Supervisory Board of the Bank shall determine prohibitions/restrictions on certain types of activities and/or attract certain types of clients by the Customer Acceptance Policy.

3.3. Risk appetite indicators that the Bank considers unacceptable are:

3.3.1 Any criminal activity, manifestations, facts, assumptions based on the results of analysis of available information and may indicate that a financial operation or its participants, their activities or the origin of assets are related to ML/FT, or with commitment of another criminal offense or act, for which international sanctions are applicable, including the criteria determined by the AML/CFT Law and the NBU Regulation on AML/CFT issues.

3.3.2 Maintaining business relationships / conducting financial operations with clients and/or their counterparties which belong to the lists of prohibitions (restrictions) stipulated by this AML/FT Policy and the Customer Acceptance Policy.

3.4 According to risk-based approach, the Bank shall reserve the right to refuse the client (person) to establish/maintain business relationships, conduct financial operations if such operations or activities of the clients and/or the their counterparties increase the Bank's risk of being used for illegal purposes, have indicators suspicions for the Bank or not supported by the data specified by the AML/CFT Laws.

3.5 The Bank shall refuse to establish (maintain) business relationships / to open accounts (provide services) for persons (clients), including by terminating business relationships, closing accounts / refusing to conduct financial operations (including those conducted without establishing business relationships) in the cases, as follows:

- if the client is classified as person with whom cooperation is prohibited or restricted by the Customer Acceptance Policy or the AML/CFT Policy (including

the Bank's Sanction Policy, which is specified in Section 6 of the AML/CFT Policy);

- if the client's identification and/or verification, as well as determination of data for ultimate beneficiaries identification are impossible or the Bank has a reason to believe that the client's UBO is a commercial agent, nominee owner or nominee holder, or intermediary of the property rights of another person;

- if there are doubts whether the person acts in his/her own behalf, represents falsely oneself to be another person, illegally appropriating someone else's identification data, or acting on behalf of other persons (beneficiary, beneficiaries), without legal grounds;

- if the identification of a person on behalf of or in the interests of whom the financial operation is being conducted, and identification of his/her UBO or beneficiary in the financial operation is impossible;

- if a person's manifestations, attempts or facts of suspicious financial operation and/or suspicion of financial fraud, political corruption, use of the Bank's accounts/services with the ML/FT purpose or for committing another criminal offense specified by the Criminal Code of Ukraine are revealed;

- if a person intends, displays or attempts to commit deliberate or intentionally negligent violation of the Ukrainian legislation or the Bank's internal procedures, does not comply with the Bank's legal requirements to provide documents/information specified by the law and/or otherwise expresses his/her disrespect and disloyalty to the legislation of Ukraine and/or internal procedures of the Bank;

- if a client failed or refused to provide, at the Bank's request, any documents or data necessary for identification and/or enhanced CDD/EDD;

- if a client or his/her representative provided inaccurate information or any information meant to mislead the Bank;

- if regarding a client was established an unacceptably high risk;

- if a correspondent financial institution is a shell bank and/or maintains a correspondent relationship with the shell bank;

- if a person is a shell company, trust, or company that issued bearer shares, or is an institution that is not a subject to regulation and licensing by government authorities and is not a subject to their supervision, including: by money transfer agent, exchange office, cash desk/currency exchange office, etc.

3.6 The Bank shall determine a potential possibility of being a subject to penalties by the NBU, and at the same time, the extent to which the Bank accepts control

deficiencies cannot exceed the norms and requirements specified in this AML/CFT Policy.

In case of corrective measures application, the Bank, as soon as possible, shall ensure creation and implementation of an action plan to correct the identified violations and deficiencies.

4. Requirements to the Bank's Internal AML/CFT Documents

4.1 The Bank shall carry out its AML/CFT activities in accordance with the recommendations and standards adopted by the Financial Action Task Force on Money Laundering (FATF), in particular, the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation of weapons of Mass Destruction (hereinafter - FATF Recommendations), the principles developed by the Wolfsberg Group, the requirements of the Basel Committee on Banking Supervision, AML/CFT Laws of Ukraine, regulations of the National Bank of Ukraine and the Ministry of Finance of Ukraine, the results of national risk assessment and risk profile of the Bank, the NBU recommendations and FIU typological studies.

4.2 The Bank shall perform its activities in strict compliance with the Local AML/CFT Laws, namely:

- Law of Ukraine "On Prevention and Counteraction to Legalization (Laundering) of Proceeds from Crime, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction" (hereinafter - the AML/CFT Law);
- Law of Ukraine "On Banks and Banking";
- Law of Ukraine "On Sanctions";
- Regulation On Financial Monitoring Carried out by Banks, approved by the NBU Resolution No. 65 dated May 19, 2020 (hereinafter - the AML/CFT regulatory legal act;
- Resolution of the National Bank of Ukraine dated October 01, 2015 No.654 "On Implementation and Monitoring of the Effectiveness of Personal Special Economic and Other Restrictive Measures (Sanctions)";
- other laws of Ukraine regulating the AML/CFT issues, regulations of the National Bank of Ukraine, Cabinet of Ministers of Ukraine, Ministry of Finance of Ukraine adopted for the implementation and pursuant to the above laws;
- recommendations of the State Financial Monitoring Service of Ukraine (Financial Intelligence Unit, FIU), in particular the typological studies published on its official webpage;
- recommendations of the National Bank of Ukraine published on its official webpage.

4.3 To comply with the Local AML/CFT Laws, the Bank, according to the legislation requirements, the results of the national risk assessment and risk assessment inherent in its activities, has developed and implemented rules for financial monitoring, programs for primary financial monitoring and other related internal documents (hereinafter - internal AML/CFT documents), which take into account the specifics of the Bank's activities, its clients' characteristics, as well as the RBA implementation.

4.4. The Bank's internal AML/CFT documents include the following procedures:

- implementation of CDD/EDD measures (including those for UBO identification and verification, business relationships and financial operations monitoring, customer data update, etc.);
- PEPs identification and procedures for application of additional measures to them;
- valuation / revaluation of the Bank's and clients' risk profiles and taking measures to mitigate ML/FT risks;
- identification of ML/FT risk criteria and suspicious financial operations indicators;
- taking necessary additional measures to establish a correspondent relationship with a foreign financial institution;
- maintaining an electronic questionnaire to ensure timeliness, completeness and accuracy of the information on clients;
- refusal to establish (maintain) business (contractual) relationships / accounts opening (servicing), including through business (contractual) relationships termination, accounts closure / refusal to conduct financial operations in cases provided by the AML/CFT Law;
- identification of discrepancies between the information on UBO in the Unified State Register of Legal Entities, Individuals - Entrepreneurs and Public Associations, and information received by the Bank as a result of the customer due diligence;
- application of the imposition tools (information obtained from a third party as defined by the AML/CFT Law) in case the Bank decides to use such tools;
- involvement of agents, organization of trainings for them (their employees) and their activities control;
- entering a relevant information with notification registers;
- use of automation systems, the list of which is defined by the AML/CFT Regulation;

- information exchange with FIU and implementation of its relevant decisions / instructions;
- freezing the assets related to terrorism and its financing and proliferation of weapons of mass destruction and its financing;
- suspension of financial operations in cases specified by the AML/CFT Law;
- funds transfer support with relevant information pursuant to requirements specified in the Article14 of the AML/CFT Law;
- relevant limits control in case of using SDD during identification and verification of a client (representative thereof);
- ensuring the secrecy of financial monitoring, and confidentiality of other information;
- informing the Security Service of Ukraine in cases specified by Ukrainian AML/CFT legislation;
- conducting the Bank's AML/CFT staff training;
- staff familiarization with the Bank's internal documents regulating AML/CFT;
- retention of all documents / information related to the Bank's compliance with the requirements of the Ukrainian AML/CFT legislation.

All internal AML/CFT documents shall include the list of the Bank's structural units, employees responsible for CDD/EDD/SDD measures, and allocation of responsibilities between them.

4.5 The Bank's rules, programs and other internal AML/CFT documents are documents with restricted access.

5. The Bank's AML/CFT Trainings

5.1. AML/CFT training shall be mandatory for all categories of bank employees involved in the relevant defense measures, and shall be adapted to specific activities of the Bank as well. The objective of such training is to develop an in-depth understanding of the Bank's expectations, and job responsibilities / roles in the area of AML/CFT by the employees.

5.2. The AML/CFT staff training envisages the annual preparation and implementation of plans for AML/CFT training, which include:

- intrabank trainings (developed and conducted at the expense of the Bank's internal human resources and/or with the involvement of external lecturers / teachers);

- external trainings (the Bank's employees are scheduled to attend external AML/CFT trainings / appropriate certifications);

- the Bank's employees familiarisation with the Local AML/CFT Laws and international documents, liability for violation of the AML/CFT legislation requirements, and ensuring that the acquired knowledge is verified by regular testing to control the level of knowledge expected;

- practical trainings in the implementation of internal AML/CFT requirements, including aspects of working with the software modules available in the Bank in order to comply with the legislation and internal documents requirements;

- familiarisation with the highest risk zones of the Bank based on the results of its risk profile assessment, examples of violations by banks, other persons' relevant sanctions.

5.3. The AML/CFT trainings shall also include:

- creation of permanently available mechanisms for consultations on AML/CFT issues,

- empowering employees to notify on policy or control aspects which they consider insufficiently clear / useful / efficient;

- studying the best practices regarding detection of clients' financial operations which may be associated with AML/CFT (typologies, schemes);

- employees' mandatory familiarization with the requirements of the AML/CFT intrabank documents prior they begin to perform their job duties (including in the event of their significant change) and in the event of amendments to the AML/CFT intrabank documents.

5.4. The Bank shall take measures in accordance with the local AML/CFT legislation to ensure that the responsible employee completes the AML/CFT training. The Bank's training programs shall include training on international AML/CFT standards and trends conducted at least once a year for the Bank's managers, employees of the AML/CFT and internal audit units.

5.5. The Bank shall regularly provide staff trainings regarding identification of suspicious financial operations, escalation / information procedures (including its suspicions, possible violations, identified indicators of suspicious financial operations, risk criteria, and other AML/CFT problematic issues) available in the Bank.

5.6 The Bank's employees shall be trained mostly through e-learning courses formed at their workplaces.

The employees who completed an appropriate training shall be tested for the level of knowledge. Those who received unsatisfactory test results shall take repeated training

courses.

5.7. The Bank shall document the facts of the relevant training.

6. Sanctions Policy of the Bank

6.1 The purpose of the Bank's Sanctions Policy is to ensure compliance of the Bank operations with the AML/CFT legislation, the Law of Ukraine "On Sanctions", organization and functioning of the internal AML/CFT risk management system minimizing the risks of avoiding restrictions imposed by special economic and other restrictive measures (sanctions) (hereinafter – sanctions) and makes it impossible to use the Bank's products and services to launder proceeds from illegal activities, terrorism financing or conducting operations which promote or may promote the avoidance of sanctions.

6.2 For the purposes hereof, the Bank means sanctions as the measures taken by the State of Ukraine and other national governments, intergovernmental bodies, which commited to change the behavior and/or actions of a foreign state, foreign legal entity or individual, or other entities posing real and/or potential threats to the interests, security, sovereignty and territorial integrity of the countries, contribute to terrorism activities and/or violate the rights and freedoms of a person and citizen, the interests of the society and the state, lead to occupation of the territory, expropriation or restriction of the right to property, infliction of property damage, creation of obstacles to sustainable economic development and the full enjoyment of rights and freedoms by citizens.

The Bank shall take into account the sanctions recognized by Ukraine in accordance with the international treaties of Ukraine or decisions of interstate associations, international and intergovernmental organizations to which Ukraine is a party, foreign states (in accordance with the procedure determined by the Cabinet of Ministers of Ukraine) regarding freezing the assets of certain persons or restricting their access to them, as well as sanctions adopted in accordance with the Bank's internal assessment (in accordance with approved internal orders and instructions) to implement the decision, resolution, statement, recommendations of international and intergovernmental organizations, in particular, those carrying out activities in the field of ML/FT, including assets freezing, prohibitting funds remittance, conversion, investment, as well as flow of assets related to terrorism and its financing, proliferation of weapons of mass destruction and its financing.

6.3 To enforce the Sanctions Policy, the Bank shall use:

- a decision on the application, cancellation or amending sanctions against a foreign state or general public with a certain type of activities (sectoral sanctions) adopted by the National Security and Defense Council of Ukraine and enacted by a decree of the President of Ukraine (hereinafter – the "NSDCU sanctions")

- a list of terrorists;

- a list of states (territories) not implementing or improperly implementing the

recommendations of international and intergovernmental organizations active in the field of combating the ML/FT, which is formed and approved in accordance with the procedure established by the laws of Ukraine;

- the resolutions of the United Nations (UN) General Assembly and Security Council;
- the decisions and regulations of the Council of the European Union (EU);
- the lists of the Office of Financial Sanctions Implementation (OFSI) of Her Majesty's Treasury (HM Treasury) of the Great Britain;
- the lists of states sponsoring terrorism, in particular as defined by the U.S. Department of State;
- the Financial Action Task Force (FATF) statements on the countries which do not comply with the AML / CFT;
- the reports from the Office of Foreign Assets Control (OFAC) of the U.S. Treasury Department;
- a list of networks for combating financial crime USA (FinCen);
- a list of the Ministry of Finance of Japan (MOFJ);
- Canadian sanctions related to Ukraine [DFATD (Canada) Special Economic Measures (Ukraine) Regulations];
- other official lists related to terrorist activities, decisions acceptable to the Bank regarding assets freezing, prohibitting funds remittance, conversion, investment, as well as flow of assets related to terrorism and its financing, proliferation of weapons of mass destruction and its financing, to which there is a prohibition for financing, participation and any other actions, which are or may be related to sectoral sanctions applicable to specific activities and/or economies of the states concerned.

6.4 The Bank shall not establish business (contractual) relationships, shall not credit or transfer funds and/or carry out other financial operations with assets and/or other actions provided for in the sanctions restrictions, if a client [a client's representative and/or participant (founder, shareholder), and/or a client's UBO, and/or participant, and/or beneficiary of a financial operation (hereinafter – the related persons)] and/or the institution through which the transfer (receipt) of assets is carried out, and/or related persons of this institution are included in:

- the lists of specifically designated persons subject to personalized sanctions, which are formed and maintained by the Office of Foreign Assets Control (OFAC) of the U.S. Department of Treasury (hereinafter – the SDN List);

- a consolidated list of the UN Security Council;
- consolidated list of persons, groups and entities subject to EU financial sanctions;
- a list of the OFSI HM Treasury of the Great Britain;
- a list of persons subject to personal special economic and other restrictive measures (sanctions) adopted by the relevant NSDCU decision and enacted by the relevant decree of the President of Ukraine;
- a list of terrorists, their representatives acting on behalf of persons included in the List of terrorists, legal entities owned (directly or indirectly) by persons included in the List of terrorists and/or governing bodies represented by persons included in the List of terrorists;
- a list of certain activities of persons subject to a prohibition on funding, participation and any other actions, which are or may be related to the sectoral sanctions as applied to specific activities and economies of the states concerned (hereinafter – the SSI List).

6.5 The Bank shall not establish business (contractual) relationships, shall not credit or transfer funds and/or carry out other financial operations with assets and/or other actions provided for in the sanctions restrictions, if a client and/or its related persons (including a diplomatic mission, an embassy, or a consulate of a foreign state) and/or the institution through which the assets are transferred (received), and/or the country of origin of goods and/or transit territory of goods/services have a relevant registration, place of residence (domicile), location or country (territory) of origin, which:

- is included in the list of States (territories), which do not implement or improperly implement the recommendations of international and intergovernmental organizations engaged in AML/CFT activities, which is formed and approved in accordance with the procedure established by the laws of Ukraine;
- do not comply with AML/CFT requirements in accordance with the statements of the Financial Action Task Force (FATF);
- is selected in accordance with the Bank's RBA internal assessment, including, but not limited to the countries with a respective share of SDN persons from the total number of personal sanction restrictions under all programs;
- is recognized by the U.S. Department of State as a sponsor of terrorism or subject to enhanced U.S. control;
- is an unrecognized state / territory / political entity possessing the basic attributes of statehood, but deprived of international recognition.

6.6 The Bank shall carry out an enhanced due diligence with respect to clients / their financial operations with assets, if the clients and/or their related persons (including a diplomatic mission, an embassy, or a consulate of a foreign state), and/or the institution through which the assets are transferred (received), and/or the country of origin of the goods and/or transit territory of goods / services have a relevant registration, place of residence (domicile), location or country (territory) of origin, which:

- has strategic deficiencies in the field of counteraction to the legalization (laundering) of proceeds of crime, terrorism financing and financing of proliferation of weapons of mass destruction in accordance with the statements of the Financial Action Task Force (FATF);

- is determined in accordance with the Bank's RBA internal assessment, including, but not limited to, the countries with a respective share of SDN persons from the total number of personal sanction restrictions under all programs;

- is not implementing or improperly implementing the recommendations of international and/or intergovernmental organizations for combating the legalization (laundering) of proceeds of crime, terrorism financing and financing of proliferation of weapons of mass destruction;

- is a state that by any means has occupied a part of the territory of Ukraine or is committing aggression against Ukraine, and is recognized by the Verkhovna Rada of Ukraine as an aggressor or occupier state;

- is included in the list of offshore zones by the Cabinet of Ministers of Ukraine;

- supports terrorism, is a subject to sanctions, embargoes or similar measures in accordance with UN Security Council resolutions and/or laws of Ukraine;

- is a country identified by the European Commission as having a weak anti-money-laundering and counter-terrorism financing regime;

- is a country with an increased risk of corruption according to the Transparency International;

- is a country with an increased risk of terrorist financing according to the Institute of Economy and;

- is included to the SSI list.

6.7. The Bank shall establish a high level of AML/CFT risk and implement EDD measures in relation to the clients and their related persons have acquired the status of persons subject to the Sanctions Policy, if a client / business partner and/or his/her related person:

- has a relevant registration, place of residence (domicile), location or country (territory) origin, as defined in clause 6.6 hereof;

- is included to the SDN list;

- is included to the List of Terrorists, ia a representative acting on behalf of persons included in the List of terrorists, legal entities owned (directly or indirectly) by persons included in the List of terrorists and/or governing bodies represented by persons included in the List of terrorists;

- is included to the NSDCU Sanction List;

- is included to the SSI list.

The Bank shall be entitled to establish an unacceptably high risk (with the subsequent application of relevant restrictive measures) and refuse to maintain business relationships (including by termination of business relationships) with the persons specified in this clause.

The Bank shall be entitled to revise the list in accordance with amendments to sanctions and/or RBA.

6.8 The Bank shall introduce the relevant controls to implement the Sanctions Policy, which include, but not limited to:

- refusal to establish business relationships with the persons included in the sanctions lists;

- monitoring (screening) of the customer database, which involves a real-time detection of indicators of connection with the persons from the List of Terrorists before establishing a business relationship with a client, conducting financial opeartions, as well as regular reviewing of information available in the customer database and ensuring that all customers, including individuals, legal entities, founders, shareholders and clients' UBOs are registered in the Bank's databases, and are screened against the relevant sanctions lists of designated individuals, groups and organizations;

- monitoring (screening) of the customer data when amending sanctions lists stipulated by the Sanctions Policy;

- EDD measures regarding the existing business relationships with clients included in the sanctions lists and their related persons, restrictions on cooperation with clients (including by termination of business relationships) subject to sanctions (international and/or local);

- measures to verify the financial operations, payments and transfers are integrated into the Bank's IT systems to ensure compliance with the sanctions controls;

– measures to stop (freeze assets) financial operations related with the persons and financial liabilities to the persons included in the sanctions lists in accordance with the established sanctions requirements.

6.9 The Bank shall refuse to carry out financial operations, if they:

– are intended, contribute or may contribute to the avoidance of restrictions imposed by sanctions;

– violate, contribute or may contribute to the violation of sanctions restrictions.

6.10 The Sanctions Policy shall apply to:

– individuals / individual entrepreneurs - clients of the Bank (representatives thereof) who are citizens having registration, place of residence (domicile), or location in the relevant state (territory) (including those having a refugee status);

– legal entities - corporate clients of the Bank, who are registered or located in the relevant country (territory);

– founders (participants, shareholders) – legal entities (corporate clients), who directly and/or indirectly own 10 percent and more of the authorized capital and/or voting rights under shares, or units of the legal entity, or have the opportunity to significantly influence the management or activities of the legal entity regardless of formal ownership;

– UBOs of corporate clients - legal entities;

– correspondent banks with which the Bank establishes correspondent relationships;

– institutions through which the client / client's counterparty transfers assets and its founders (participants, shareholders) who directly and/or indirectly independently or jointly with other persons own 10 percent and more of the authorized capital and/or voting rights under shares, units of the legal entity, or have the opportunity to significantly influence the management or activities of the legal entity regardless of formal ownership, their UBOs;

– business partners of the Bank.

The Bank shall be entitled to take into account individual peculiarities in respect of clients who are residents of the countries (territories), the list of which is provided in the clauses 6.5 and 6.6 hereof, and to establish specific service regimes for them.

7. Final Provisions

7.1. This Policy shall come into effect since it is approved by the decision of the Supervisory Board and shall be communicated to and implemented by the Management Board and the employee responsible for financial monitoring at the Bank.

7.2. The Bank shall ensure that the amendments to the AML/CFT Policy to be introduced in accordance with the laws of Ukraine, as well as the best international and domestic AML/CFT practices.

The amendments to the AML/CFT Policy shall be approved by the decision of the Supervisory Board through issuing the restated wording.

7.3. In the event of amendments to the laws and/or the Articles of Association, the AML/CFT Policy provisions shall be effective to the extent they do not contradict the laws of Ukraine and/or the Articles of Association.

7.4. The Bank shall introduce the procedures and rules aimed at implementation of the requirements set forth in this AML/CFT Policy.