Joint-Stock Company Commercial Bank "PrivatBank"

COMPLIANCE FUNCTION

APPROVED
decision of the Supervisory Board
Minutes No. 24/19 dated 21/11/2019

Policy of prevention and counteraction to legalization (laundering) of proceeds of crime, terrorism financing and financing of proliferation of the mass destruction weapons

Registration number: 2019/7278275
Document status: opened
Approval data:
decision of the Board of the Bank, Minutes No. 45 dated 28.10.2019

Kyiv city

JSC CB "PrivatBank"
Policy of prevention and counteraction to legalization (laundering) of proceeds of crime, terrorism financing and financing of proliferation of the mass destruction weapons

Contents

1. General AML/CFT Rules and Standards of the Bank

1.1. This Policy adopted by JSC CB "PrivatBank" on matters concerning regulatory compliance in the area of prevention and counteraction to legalization (laundering) of the proceeds of crime, terrorism financing and financing proliferation of weapons of mass destruction (hereinafter referred to as the Policy) applies to the divisions of JSC CB "PrivatBank" (hereinafter referred to as the Bank), including separate divisions and those situated in other jurisdictions, to the Bank's employees, business partners, participants of groups/payment systems of which the Bank is a member, to customers enabling financial transactions with the Bank's support in the territory of Ukraine and beyond in keeping with international treaties entered into by Ukraine and consented to by the Supreme Council of Ukraine (Verkhovna Rada) as binding, and to their counteragents.

1.2. The Policy's main task is to prevent the use of the Bank's services for the purpose of money laundering, terrorism financing and financing proliferation of weapons of mass destruction (hereinafter referred to as AML/CFT) and to prevent any other activities preceding or contributing to AML/CFT.

The Policy describes basic AML/CFT rules and standards of the Bank which all Bank employees shall observe in order to ensure strict compliance with the laws of Ukraine in the AML/CFT area (hereinafter referred to as Local AML/CFT Laws) and international standards.

1.3. The main AML/CFT tasks of the Bank include:

1.3.1. Adequate management of AML/CFT risks and taking relevant action in a manner and scope assuring efficient risk minimization irrespective of the risk level.

1.3.2. Implementation and application in the Bank's operations of Local AML/CFT Laws and international requirements using the risk-oriented approach (hereinafter referred to as RBA).

1.3.3. Assuring proper verification and due diligence of persons with which the institution enters into business (contractual) relations or to which it provides banking services (hereinafter referred to as CDD) enhanced due diligence measures for customers the business relationships with whom (financial transactions without establishing business relationships) constitute a high risk (hereinafter – the EDD). EDD measures are proportional to the identified risks and are aimed at their effective minimization, including by increasing the frequency and scope of monitoring the business relations and collecting additional information on business relations.

1.3.4. Reporting to the central executive body implementing the state policy of Ukraine in the area of AML/CFT to the Financial Intelligence Unit of Ukraine (hereinafter referred to as FIU) about threshold financial transactions and/or suspicious financial transactions/activities undertaken by customers, and about financial transactions reasonably suspected to be associated with, related to or designated for terrorism

financing or financing proliferation of weapons of mass destruction, and/or about attempted transactions of this kind.

1.3.5. Preventing violations in the Bank's operations of the Local AML/CFT Laws and laws effective in other jurisdictions, in particular at the time of opening correspondent accounts with foreign banks and/or during other operations of the Bank in these jurisdictions.

1.4. The Bank has adopted the following AML/CFT standards:

1.4.1. Diligent adherence to all special AML/CFT requirements, rules and principles prescribed by the Local AML/CFT Laws and international banking standards.

1.4.2. Unwavering compliance with the requirements and restrictions, as well as bans associated with AML/CFT requirements set forth in local and international requirements.

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

1.4.4. Continuous use of all available means, methods and techniques to avoid being involved in suspicious or illegal business (money laundering, fraud, activities of terrorism 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 CDD/EDD actions consistent with the level of risks determined/identified over profit-making or obtaining benefits from customer attraction or servicing. Understanding that KYC efforts the customer is essential for the Bank to provide highest quality services.

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

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

1.5. The Bank's main AML/CFT priorities are:

1.5.1. Protecting the lawful interests of citizens, the society and the State against damage which may be caused by criminal actions in the area of AML/CFT.

1.5.2. Taking all reasonable efforts to prevent any connections (including indirect ones) with money laundering, fraud or terrorism financing.

1.5.3. Careful adherence to AML/CFT rules and instructions designed to protect the Bank's image, reputation and keep the trust of customers.

1.5.4. Awareness that any violation of laws, internal regulations or 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 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 means 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 of the Bank's operations (hereinafter referred to as the National Bank), FIU and the central executive authority in charge of formulating and enforcing the State's AML/CFT policy (hereinafter referred to as the Ministry of Finance).

In order to determine (identify) AML/CFT risks (threats), the Bank takes an active part (as necessary) in the national risk evaluation actions undertaken by state financial monitoring entities, authorized government authorities in order to prevent and/or mitigate negative risk impact.

1.7. Abbreviations used herein:

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

FIU means central executive body implementing the state policy of Ukraine in the area of prevention and counteraction to legalization (laundering) of the proceeds of crime, terrorism financing and financing proliferation of weapons of mass destruction;

RBA (risk-based approach) risk-oriented approach in the area of prevention of legalization (laundering) of the proceeds of crime, terrorism financing and financing proliferation of weapons of mass destruction;

CDD means proper verification and due diligence actions regarding persons with which the institution enters into business (contractual) relations or to which it provides banking services;

EDD (enhanced due diligence) means enhanced due diligence measures for customers the business relationships with whom (financial transactions without establishing business relationships) constitute a high risk, proportionate to the risks identified and aimed at minimizing them effectively, including by increasing the frequency and scope of business relationship monitoring activities and collection of additional information about the business relationship;

KYC means Know Your Customer Policies;

PEPs means 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 countries concerned.

2. Bank documents governing the AML/CFT requirements

2.1. The Bank carries 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 pursuant to the International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (hereinafter referred to as 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 adopted for the implementation of and pursuant to the above laws which the Bank implements in order to assure the operation of its internal AML/CFT system.

2.2. Specifically, while conducting its operations the Bank provides for stringent compliance with the Local AML/CFT Laws, namely:

Law of Ukraine "On prevention and counteraction to legalization (laundering) of the proceeds of crime, terrorism financing and financing proliferation of weapons of mass destruction" (hereinafter referred to as the AML Law);

Law of Ukraine "On Banks and Banking" (hereinafter referred to as the Bank Law);

Law of Ukraine on Sanctions;

Regulation on Financial Monitoring Carried out by Banks, approved by Order of the National Bank of Ukraine Board No.417 as of June 26, 2015 (hereinafter referred to as the Financial Monitoring Regulation);

Criteria of risks related to legalization (laundering) of the proceeds of crime, terrorism financing and financing of proliferation of weapons of mass destruction, approved by Order of the Ministry of Finance of Ukraine No.584 as of July 08, 2016;

Resolution of the National Bank of Ukraine dated October 01, 2015 No. 654 on Ensuring the Implementation and Monitoring of the Effectiveness of Personal Special Economic and Other Restrictive Measures (Sanctions);

other laws of Ukraine governing the AML/CFT issues, regulations of the National Bank, Cabinet of Ministers of Ukraine, Ministry of Finance and FIU adopted for the implementation of 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 the Unit's official webpage;

recommendations of the National Bank published on the official webpage.

2.3. To comply with the Local AML/CFT Laws, the Bank's Management Board has approved and implemented rules, procedures, management measures and controls designed to prevent the Bank's use for AML/CFT purposes and for primary financial monitoring. These are reflected in internal financial monitoring documents, namely:

Financial Monitoring Rules of the Bank;

Customer Identification, Verification and Due Diligence Program of the Bank;

Program for Managing the Financial Monitoring Compliance Risk;

Financial Monitoring Program for specific customer service areas;

Financial Monitoring Program for money transfer transactions with the use of payment systems (including the use of electronic payment means) and during transactions with electronic funds using a payment system of which the Bank is a member/participant;

Training and Advanced Training Programs for Bank employees;

other documents, including the Bank's Anti-Corruption Program.

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

The Bank takes steps to prevent disclosure of information submitted to the FIU and of other financial monitoring information (including data about such information submission or about receipt of queries, decisions or instructions from the FIU and implementation thereof), excluding cases described in the Local AML/CFT Laws.

3. Application of the Risk-Based Approach in AML/CFT by the Bank

3.1. The Bank implements AML/CFT procedures using the RBA (role-based access), which provides for continuous identification (detection), (re)valuation and understanding of the AML/CFT risks, as well as for preventing and mitigating risks in a manner and scope assuring efficient minimization of the risks irrespective of their level.

RBA (role-based access) estimate makes it possible to measure the impact of AML/CFT risks on the Bank and to analyze the information received in order to understand the probability of risks and their impact both on the Bank and the banking industry at large.

To assure its compliance with the prescribed requirements, the Bank, subject to RBA (role-based access), duly distributes its resources and arranges a system of internal controls.

The Bank's internal and separate structural divisions must ensure the implementation of internal bank policies and procedures designed to terminate and identify AML/CFT occurrences.

RBA (role-based access) has been implemented in the Bank in the following way:

3.2. Appointment of a competent employee in charge of AML/CFT in the Bank (hereinafter referred to as the Compliance Officer) who is a member of the Bank's executive body, has an impeccable business reputation (allowing a conclusion on the person's compliance with applicable laws, as well as absence of prior convictions not expunged or removed from official records in keeping with the procedure set forth in the law), meets the criteria of professional and occupational aptitude, has personal qualities and skills necessary

to assure AML/CFT compliance by the Bank. The Compliance Officer shall be independent in his/her activities and shall be accountable to the Bank Manager only.

The Management Board member - Compliance Officer shall provide:

the Chairman of the Bank's Management Board with written monthly reports about AML/CFT measures implemented by the Bank;

the Bank's Management Board with reports concerning measures implemented to comply with AML/CFT requirements. The Bank's Management Board shall pass decisions on the Bank's Compliance Officer proposals submitted to assure the Bank's compliance with Local AML/CFT Laws. If the Board declines proposals submitted by the Compliance Officer, the latter shall refer to the Bank's Supervisory Board for the purpose of passing decisions declined by the Management Board.

the Bank's Supervisory Board, at least once per year, with reports on the outcomes of AML/CFT measures implemented by the Bank.

The Compliance Officer shall have relevant authorities, status, resources, experience and knowledge to perform his/her functions, including the opportunity to access all relevant internal information of the Bank. The nominee for this position shall be approved by the National Bank in keeping with the procedure set forth in applicable financial monitoring regulation.

3.3. Involvement in AML/CFT of experienced and trusted staff checked at the time of employment for professional aptitude, impeccable business reputation and trustworthiness. Functional duties are distributed between such employees in accordance with internal financial monitoring documents and job instructions. The employees are provided with adequate technical means to enable them to perform the job, proportional to the complexity of banking transactions.

3.4. Implementation of controls over the Bank employees' compliance, within the functional duties identified in the job instructions, with the requirements towards proper KYC/CDD/EDD efforts, customer due diligence, identification (detection) and (re)evaluation of AML/CFT risks, customer risk monitoring, identification of financial transactions which are subject to financial monitoring or are reasonably suspected to be associated with, related to or designated for terrorism financing or financing proliferation of weapons of mass destruction.

3.5. Approval by the Bank of policies, rules, procedures, regulations which incorporate a set of internal controls to mitigate AML/CFT risks and include but are not limited to:

3.5.1. Organizational measures assuring the functioning of a structural AML/CFT division as part of the Bank's management structure, provisions for clear distribution of functional duties among the division's employees and for segregation of their responsibilities in the AML/CFT area. Subordination of this division directly to the Bank's Compliance Officer. Charging the division with AML/CFT risk management and control, design and implementation of AML/CFT risk criteria, provisions for identification and recording of financial transactions subject to financial monitoring, submission to the FIU of information about financial transactions which are subject to financial monitoring or are reasonably suspected to be associated with, related to or designated for terrorism financing or financing proliferation of weapons of mass destruction, providing the FIU with additional information and data in response to foreign countries' requests, information regarding tracking (monitoring) of customers' financial transactions, and implementation of other actions envisaged in the AML Law.

3.5.2. Assuring that the Compliance division makes an overall assessment of the efficiency of the Bank's policies and procedures, business processes, products (services) and customer types, designed to identify, evaluate and monitor AML/CFT risks, accompanied by opinions as to the adequacy of measures taken by the Bank to manage AML/CFT risks. These opinions shall be brought to the attention of the Bank's Management Board on a monthly basis and the Supervisory Board on a quarterly basis. Identification of tasks based on the findings of risk identification and classification evaluation, control of activities implemented and giving proposals as to the scope of AML/CFT measures and resources required to mitigate the risks.

3.5.3. Implementation of controls by employees of the Bank's business divisions (including with regard to processes associated with cross-border transfers) designed to identify attributes or a set of attributes of suspicious financial transactions, their participants and their intentions/actions undertaken to conceal actual beneficiaries and/or any other actions associated with acquisition, ownership or use of assets (funds) which may be obtained through perpetration of crimes committed to conceal or disguise the sources of these assets (funds).

3.5.4. Audits performed at least once per year by the Internal Audit Unit to verify compliance with the AML/CFT laws, including audits of the adequacy of measures implemented by the Bank to manage

AML/CFT risks. Preparation of opinions and proposals based on such audits which shall be considered by the Bank's Supervisory Board, and control over actions to address the violations identified.

3.6. Implementation of the process designed to track (monitor) risk criteria based on the geographic location of the customer's registration country or of the institution via which the customer transfers (receives) assets, based on the goods or service type, service provision (receipt) method, also taking into account the risk-bearing financial transactions conducted by customers and their regularity. Documentation of the aggregate risk analysis findings, evidencing the probability of the Bank's services being used by its customers for AML/CFT, continuous updating of those findings and bringing them to the attention of relevant persons in charge. Regular submission of the Bank's risk estimates and measures taken to mitigate the same to the Bank's Management Board.

3.7. Implementation of preventive actions which provide for:

3.7.1. Segregation and classification of customers based on their placement in AML/CFT risk groups: low, medium, high and unacceptably high risk levels. Assignment of unacceptably high risk for any customer or financial transaction if the Bank may not reasonably monitor or reduce extreme risks associated with this customer or financial transaction, or if following customer due diligence there are reasons to believe that the declared business activities of the customer and/or its financial transactions contain fictitious signs.

3.7.2. Refusal to establish (maintain) business (partner) relations, suspension/refusal of financial transactions to prevent, restrict AML/CFT risks and/or reduce the same to an acceptable level.

3.8. Performance, taking into account RBA (risk-based approach) of documented checks of the sources of funds (assets) associated with financial transactions, obtaining data regarding the origin of such assets enabling a clear understanding of the sources of fortune (wealth), customer's title to own/dispose of the same (rights to the same), amount/size of aggregate assets (fortune) of the person and the history of obtaining (accumulation) thereof. The outcomes of the above checks are recognized as adequate subject to the availability of documented proof of the customer's financial capacities which, when disposed of, allow the performance or initiation of financial transactions involving relevant amounts.

3.9. Implementation of RBA (risk-based approach) actions designed to identify financial transactions subject to financial monitoring which includes continuous analysis of financial transactions in order to determine the essence and purpose of financial transactions, issue of opinions on the correspondence/non-correspondence of financial transactions to the customer's financial standing and/or nature of their operations, regularity of financial transactions conducted etc. Thorough investigation of grounds and purposes of all complex and unusually large financial transactions, all unusual schemes of financial transactions with no economic viability (sense) and/or legal purpose, and/or non-conforming to the customer's financial standing and/or nature of operations.

3.10. Continuous implementation procedures to identify and revaluate AML/CFT risks which provide for comparison of information received during the analysis of the customer's financial transactions against the information received at the time of establishment of business (contractual) relations (including in the course of updating the data related to identification, nature of operations and financial standing), and against the information received during the preceding service periods.

3.11. Management of AML/CFT risks associated with the implementation or application of new and existing information products, business practices or technologies, including those facilitating financial transactions without direct customer contacts.

3.12. Assuring the monitoring, detection and recording of customers' financial transactions (including those conducted in favor of customers) to check such financial transactions against the information available to the Bank about the customer, their activities and risks, including if necessary information about the sources of customer funds, threshold and suspicious financial transactions, and/or attempted transactions, namely with the use of automation means enabling an analysis of batches of financial transactions based on the risk criteria set for business relations (one-off financial transactions) with all customers or customer groups.

3.13. Application of the Know Your Customer (KYC) Policy in the Bank which provides for the following, among other things:

3.13.1. Due identification, verification of customers (representatives thereof), customer due diligence, updating/further updating of customer information, obtaining information about customers' counteragents, actions to obtain information and/or documents in order to establish the ultimate beneficiary owner

(controller) or its absence of the customer (hereinafter referred to as the ultimate beneficiary), financial transaction beneficiary, conducting CDD/EDD (enhanced due diligence) etc.

3.13.2. Identification, verification of customers depending on the risk of financial transactions irrespective of the threshold amounts subject to financial monitoring and irrespective of the fact whether the financial transaction is conducted a single time or as part of several financial transactions which may be interrelated.

3.13.3. Furnishing all transfers involving amounts specified in the AML Law (including transactions with foreign currency, banking metals and other assets) with information regarding transfer initiators (payers) and recipients.

3.13.4. Setting restrictions for the use of product and service provision channels where no direct contact with customers is envisaged.

3.13.5. Assuring that EDD (enhanced due diligence) based on the RBA (risk-based approach) are applied to customers, the relations with which (whose financial transactions without the establishment of business relations) pose a high risk, with the said measures being proportional to the detected AML/CFT risks and directed at the efficient mitigation thereof, including by way of increasing the frequency and scope of enhanced due diligence and monitoring of customer activities, collection of additional information regard the customer etc., as per the list provided in para.5.2.1. herein.

3.13.6. Prohibition to set up and maintain anonymous (numbered) accounts.

3.13.7. Prohibition to set up branches, other separate divisions and representative offices and prohibition to carry out any activities in countries which do not apply or apply inadequately the recommendations of the Financial Action Task Force on Money Laundering (FATF).

3.13.8. Prohibition to establish correspondent relations with financial (lending) institutions or with institutions carrying out activities equivalent to those carried out by financial or lending institutions established or incorporated in a country (territory) where they do not have a physical presence with the actual management center, and not affiliated to a regulated financial group and/or not subject to relevant supervision in the country (territory) of their location (hereinafter referred to as shell banks), or with foreign financial (lending) institutions which based on the information from independent and reliable sources allow their accounts to be used by shell banks.

3.13.9. Prohibition to establish contractual relations/open accounts for shell companies, dummy or fictitious companies created by third parties to conceal the actual beneficiary, for entities whose ultimate beneficiaries have attributes of agents, nominees (nominee holders) or are simply intermediaries regarding such title.

3.13.10. Prohibition to establish (maintain) business relations with customers and to conduct financial transactions (also without establishing business relations) in the following events:

there are doubts whether the person acts in their own name;

customer identification and/or verification (including determination of data enabling to identify ultimate beneficiaries), CDD are impossible or the Bank has doubts whether the person acts in his/her own behalf;

it is established that the customer provided inaccurate information or any information meant to mislead the Bank during identification and/or enhanced CDD/EDD (enhanced due diligence);

customer's failure or refusal to provide, at the Bank’s request, any documents or data required by the same.

3.13.11. Prohibition to establish business relations with customers and transact with persons (specifically without establishing business relations) which specified in Section 6 of the Policy (Bank Sanctions Policy).

3.14. Regular checks of the Bank's operations by the National Bank which maintains control over the activities of banks from the viewpoint of financial monitoring , taking into account supervision-related RBA.

3.15. Continuous implementation by the Bank of the actions to analyze and review the RBA (risk-based approach) based estimates, and implementation of relevant actions in the event of changes in the Bank's operations or emergence of new threats. Assessment of AML/CFT risks subject to the findings of national assessment and typological studies of the dedicated AML/CFT authority, recommendations of the National Bank and other state financial monitoring entities. Decision-making by the Bank subject to the outcomes of AML/CFT risk levels assessment, monitoring and analysis, and evaluation of the potential impact of the Bank's decisions on the AML/CFT risk levels prior to decision-making.

4. Key Requirements of the Bank's Know Your Customer Policy

4.1. The efforts implemented by the Bank include but are not limited to:

4.1.1. KYC procedures (their representatives), persons for whom or on whose behalf financial transactions are conducted, under circumstances envisaged in the Local AML/CFT Laws.

4.1.2. Actions taken to obtain information and/or documents in order to determine the ultimate beneficiary, including procedures for obtaining additional information and/or documents and precluding the establishment of contractual relations with (opening of accounts for) customers whose ownership structure is not transparent. The Bank uses the RBA (risk-based approach) pursuant to which the Bank is forbidden to establish business (contractual) relations and/or transact with customers regarding which the Bank's employees have not taken adequate measures to determine their ultimate beneficiaries, the beneficiaries of the financial transactions and/or which are reasonably suspected of engaging agents, nominees (nominee owners) or intermediaries with a view to concealing the ultimate beneficiaries.

4.1.3. Revealing the purpose and nature of future business relations with customers and documented confirmation of the findings, including without limitation the following measures:

4.1.3.1. Verification of customers entering into contractual relations with the Bank against the Lists of Persons related to terrorism activities or subject to international sanctions (hereinafter referred to as "the List of Persons") using the software enabling such checks.

4.1.3.2. Verification of customers (their representatives), founders (members, shareholders) of customers and ultimate beneficiaries against lists of customers which are subject to service restrictions, including but not limited to countries (territories) included in the lists specified in Section 6 of the Policy (Bank Sanctions Policy). In order to maintain the above lists the Bank is connected to databases operated and updated by the international companies World Check and Dow Jones.

4.1.3.3. Determining whether the customer (their representative), persons acting on their behalf, ultimate beneficiaries, persons being members of the customer's executive/management body or beneficiaries of financial transactions belong to politically exposed persons (hereinafter referred to as PEPs), or to their connected or related parties.

4.1.3.4. Revealing the sources of funds and other assets available in the customer's accounts, including sources and assets belonging to PEPs, their connected or related parties based on the documents received from them and/or information from other sources if such information is public (unrestricted), and documented confirmation of the sources of their assets and title to the same.

4.1.3.5. Collection of information to gain an understanding of the customer, their activities, scope of transactions the customer intends to conduct through consultations with the customer and documented registration of the information received.

4.1.3.6. Conducting onsite checks of identified (determined) facts which may help confirm/disprove the information received, and/or establish other facts that may impact the Bank's decision concerning the cooperation with the customer.

4.1.3.7. Comparison of customer information made available to the Bank against the information that is contained in reliable official sources of information, is publicly available and has a highly trusted status.

4.1.4. Evaluation of the customer's financial standing using specific techniques.

4.1.5. Evaluation of the customer's reputation using specifically designed criteria.

4.1.6. Implementation of measures designed to assure updating/further updating of customer information, including the data on their activities and financial standing.

4.1.7. Obtaining additional information related to identification and/or required for customer due diligence, for clarification of customer information or enhanced customer due diligence from state authorities and state registrars, exercising the right to request information from banks and other entities, as well as implementation of actions to collect such information from other sources if such information is publicly available (unrestricted).

4.1.8. Where necessary, conducting throughout the customer service period, including the enhanced CDD of the customer's members (owners, shareholders, founders) indicated in the ownership structure, as well as of the ultimate beneficiaries which includes, but not limited to:

4.1.8.1 Continuous monitoring of the customer's business relations and financial transactions undertaken in the course of such relations, in order to make sure that such financial transactions match the information about the customer, their operations and risks available in the Bank, including checks of financial transactions conducted throughout the term of business relations (including information about the sources of funds connected with financial transactions).

4.1.8.2 An enhanced analysis and examination of the grounds and objectives of all complex and/or unusually large financial transactions, all unusual financial transaction patterns not having an apparent economic justification (meaning) and/or a legitimate purpose, and/or not corresponding to the financial condition and/or content of the customer's activities, an enhanced level of monitoring of the business relationship in which the financial transactions are carried out in order to determine whether such financial transactions or business relationships are suspicious.

4.1.9 Assuring the relevancy of documents received and kept, of customer data and information. Keeping official documents, other documents and copies thereof related to identification of persons (customers, their representatives) and of persons who were refused financial transactions by the Bank, and related to customer due diligence, customer information clarification, and all documents pertaining to the contractual relations (financial transactions) with the customer (including any analytical findings obtained during customer identification and due diligence or enhanced due diligence) for at least five years following completion of the financial transaction, termination of contractual relations with the customer; keeping all necessary data about financial transactions (sufficient to track the transaction route) for at least five years after completion of the financial transaction, account closing or termination of business relations.

4.2. The efforts specified in clause 4.1 hereof is performed under the manner defined in Bank internal regulations.

4.3. When implementing specified in clause 4.1 hereof, the Bank determines the required scope of actions in accordance with the risk criteria of the customer the purpose of and nature business relations, transaction amounts, regularity or duration of business relations etc.

4.4. Subject to the RBA (risk-based approach), the Bank may apply simplified CDD measures regarding customers with a low risk of business relations (risk of conducting financial transactions without establishing business relations) is proportional to the risks identified and may provide, in particular, for the

reduction of the frequency and scope of the efforts to monitor the business relationship and collect additional information on the business relationship.

5. Key requirements of the PEP Servicing Risk Policy

5.1. Guided by the local legislation, the Bank classifies individuals who are national or foreign public officials and officials performing political functions with international organizations as PEPs. The definition of such persons is provided in the AML Law.

5.2. If a customer (potential customer) is found to be a PEP, a connected or related party of the PEP during the establishment (continuation) of relations with such persons, and also in the event of identification of customers whose ultimate beneficiaries are such persons, the Bank manages the risks associated with business relations with or transactions of such customer in the following way:

5.2.1. Assuring that such customers are assigned an assessed risk level and that CDD/EDD (enhanced due diligence) measures are implemented; in particular, the Bank implements the following measures:

assigns a high risk rating for the business relations with the customer;

identifies the sources of funds and other assets available in the customer's accounts, including sources of funds (assets), fortune (wealth), and title to such assets based on the documents received from the customer and/or information from other sources if such information is public (unrestricted), and provides for documented confirmation of the sources of assets;

takes additional action to gain a better understanding of the customer's relationship history and the financial standing of the customer or other participants of the business relations, to reveal their market background, reputation, area of operations and business segments, to account for the risks inherent in the person's activities, in particular: level of influence, scope of authorities etc.;

carefully collects and checks customer information and data, searches for additional independent and reliable sources to verify the information provided or available to the Bank, investigates additional materials (for example, unbiased unfavorable publications in the mass media);

gives due consideration to the analysis of contracts, agreements, payments, investigation of customer transactions, receipt of documents and data pertaining to customer activities, data collection with a view to gain an understanding of the customer's operations, nature and scope of transactions conducted (intended), identification of changes in the customer characteristic (e.g. in their behavior, use of products, transaction amounts), obtaining of information concerning the customer's reputation and reputational risks, including if available from public (unrestricted) sources;

instructs the Bank's security unit to collect information and data to gain a better understanding of the risk of the customer or his/her related parties being involved in criminal activities, to check the sources of funds or fortune used in the business relations in order to make sure that those are not proceeds of crime;

requests additional information, documents and data from the customer and/or other persons, takes other actions to gain an assurance that the financial transaction matches the purpose and nature of business relations;

investigates other sensitive information obtained from the customer, third parties, state authorities and other customers of the Bank;

provides for more thorough control (checking) of financial transactions, enhanced monitoring of customers' financial transactions in order to manage and/or mitigate risks, detailed analysis to make sure that the transactions match the customer's data, the nature and purpose of business relations and banking products use.

5.2.2. Obtaining the Bank's top management approvals (permits) for establishing (continuing) business relations or conducting financial transactions without the establishment of business relations.

5.2.3. Prior to or during the establishment of business relations, implementation of measures to identify sources of such persons' funds based on the documents received from other sources if such information is public (unrestricted).

5.2.5. Updating customer information at least once per year.

5.2.4. Making provisions for continuous enhanced monitoring of business relations/financial transactions of the customer.

5.3. The Bank has relevant risk management systems in place enabling it to determine whether a customer or ultimate beneficiary belongs to PEPs, or is a PEP's family member or related party. The Bank uses free search tools made available via dedicated websites which provide targeted search services, as well as commercial databases.

5.4. When analyzing financial transactions undertaken by PEPs, or by their connected or related parties, the Bank in order to identify misuse on the part of PEPs uses a list of red flags/suspicious indicators (factors) regarding PEPs and their behavior designed and published by FATF.

6. Key requirements of the Bank Sanctions Policy

6.1 The purpose of the Bank Sanctions Policy is to ensure compliance of the Bank operations with the Law on Legalization, the Law of Ukraine on Sanctions", the organization and operation of the internal AML/CFT risk management system, which minimizes the risks of circumventing the restrictions imposed by special economic and other restrictive measures (sanctions) (hereinafter – the sanctions) and makes it impossible to use the Bank products and services to launder income from illegal activities, terrorism financing or performance of transactions which pursue, promote or may promote the avoidance of sanctions.

6.2 For the purposes hereof, sanctions mean the steps taken by the State of Ukraine and other national governments and/or intergovernmental bodies, which seek to change the behavior and/or actions of a foreign state, foreign legal entity or individual, or other entities, to create 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 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 the freezing the assets of certain persons or restricting their access to them, as well as the 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 combating the legalization (laundering) of proceeds of crime, terrorism financing and financing of proliferation of the mass destruction weapons, including the freezing of assets, ban on transfer, conversion, deployment, movement of assets related to terrorism and its financing, proliferation and financing of mass destruction weapons.

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

decisions on the application, cancellation or amendment of sanctions against a foreign country or an unrestricted circle of persons with a certain type of activity (sectoral sanctions) adopted by the National Security and Defense Council of Ukraine and implemented by a presidential decree (hereinafter – the "NSDCU sanctions");

a list of persons connected with terrorism activities or subject to international sanctions, which is drawn up and maintained by the FIU in accordance with the procedure established by the Cabinet of Ministers of Ukraine (hereinafter – the List of Persons);

the list of states (territories) not implementing or improperly implementing the recommendations of international and intergovernmental organizations active in the field of combating the legalization (laundering) of proceeds of crime or terrorism financing or financing of proliferation of the mass destruction weapons, which is formed and approved in accordance with the procedure established by the laws of Ukraine;

United Nations (UN) General Assembly and Security Council resolutions; Council of the European Union (EU) decisions and regulations;

Office of Financial Sanctions Implementation (OFSI) of Her Majesty's Treasury (HM Treasury) lists;

lists of States sponsoring terrorism, in particular as defined by the U.S. Department of State;

Financial Action Task Force (FATF) statements on the countries which do not comply with laws on counteraction to legalization (laundering) of proceeds from crime, terrorism financing or financing of proliferation of the mass destruction weapons;

report from the Office of Foreign Assets Control (OFAC) of the U.S. Treasury Department;

other decisions acceptable to the Bank to freeze assets, prohibit the transfer, conversion, deployment, movement of assets related to terrorism and its financing, proliferation and financing of the mass destruction weapons, for which there is a ban on financing, participation and any other actions, which are or may be related to sectoral sanctions, as applicable to specific activities and/or economies of the countries concerned.

6.4 The Bank shall not establish business (contractual) relationship, shall not credit or transfer the funds and/or carry out the other financial transactions with assets and/or other actions provided for in the sanctions restrictions, if the customer [customer's representative and/or participant (founder, shareholder) and/or ultimate beneficial owner (controller) of the customer and/or participant and/or beneficiary of a financial transaction (hereinafter – the related persons)] is included in:

the lists of specifically designated individuals subject to personalized sanctions, compiled and maintained by the Office of Foreign Assets Control (OFAC) of the U.S. Department of Treasury (hereinafter – the SDN List)

the UN Security Council's consolidated list;

the consolidated list of individuals, groups and entities subject to EU financial sanctions;

a list of OFSI HM Treasury of the UK;

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 pf Persons;

a list of certain activities of individuals subject to a ban 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 countries concerned (hereinafter – the SSI List).

6.5 The Bank shall not establish business (contractual) relationship, shall not credit or transfer the funds and/or carry out the other financial transactions with assets and/or other actions provided for in the sanctions restrictions, if the customer and/or its related persons (including a diplomatic mission, an embassy, or consulate of a foreign country) 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:

are included in the list of States (territories), which do not implement or improperly implement the recommendations of international and intergovernmental organizations for combating the legalization (laundering) of proceeds of crime or terrorism financing or financing of proliferation of the mass destruction weapons, compiled and approved in accordance with the procedure established by the laws of Ukraine;

do not comply with requirements on combating the legalization (laundering) of proceeds of crime, terrorism financing and financing of proliferation of the mass destruction weapons in accordance with the statements of the Financial Action Task Force (FATF)

are selected in accordance with the Bank's internal assessment based on the RBA principles, 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;

recognized by the U.S. Department of State as a sponsor of terrorism or subject to enhanced U.S. control;

unrecognized states/territories/political entities possessing the basic attributes of statehood, but deprived of international recognition.

6.6. The Bank shall carry out enhanced due diligence of the customer/their financial transactions with assets, if the customer and/or a related person with the customer (including a diplomatic mission, an embassy, or a consulate of a foreign country) 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 the mass destruction weapons in accordance with the statements of the Financial Action Task Force (FATF)

is determined in accordance with the Bank's internal assessment, which is based on the RBA, 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;

fails to implement or improperly implements the recommendations of international and/or intergovernmental organizations for combating the legalization (laundering) of proceeds of crime, terrorism financing and financing of proliferation of the mass destruction weapons;

is a State that has occupied in any way 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 activities, is 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 on the SSI list.

6.7 The Bank establishes a high level of AML/CFT risk and implements EDD efforts in relation to customers and their related persons, who in the course of the servicing by the Bank have acquired the status of persons subject to the Sanctions Policy, if the customer and/or its related person:

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

is on the SDN list;

is on the List of Persons;

is on the NSDCU Sanction List;

is on 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 relations (including by termination of business relations) with the persons specified in this clause of the Sanctions Policy.

6.8 The list of countries (territories) specified in clause 6.6 hereof is posted on the official website of the Bank.

The Bank shall be entitled to revise the list in view of changes in sanctions and/or RBA.

6.9 The Bank has introduced the relevant controls to implement the Sanctions Policy, which include, but not limited to:

refusal to establish business relationship with the persons on the sanctions lists;

monitoring (screening) of the customer base, which ensures that all customers registered in the Bank databases, including the individuals, legal entities, founders, shareholders) and ultimate beneficial owners

(controllers) of the customers are screened against the relevant sanctions lists of designated individuals, groups and organizations;

EDD efforts regarding the existing business relationships with customers on the sanctions lists and their related persons, restrictions on cooperation with customers (including the termination of business relationships) subject to sanctions (international and/or local);

the efforts to verify the financial transactions, payments and transfers integrated into the Bank's IT systems to ensure compliance with the sanctions regime;

the efforts to stop (freeze assets) of financial transactions of the persons and financial commitments to the persons on the sanctions lists in accordance with the established sanctions requirements.

6.10. The Bank shall refuse to carry out financial transactions, which:

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

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

6.11 The Sanctions Policy shall apply to:

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

corporate customers of the Bank, which are registered or located in the relevant country (territory)

founders (participants, shareholders) of corporate customers, which directly and/or indirectly own 10 percent or 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;

ultimate beneficial owners (controllers) of corporate customers;

correspondent banks with which the Bank establishes correspondent relations.

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

7. Key Requirements as to the Bank's Reporting of Suspicious Financial Transactions

7.1. Subject to the Local AML/CFT Laws, the Bank shall notify the FIU about:

threshold financial transactions whose amounts and attributes are defined in the AML Law;

suspicious financial transactions (activities), accompanied with valid opinions, document copies and other information upon which the suspicions are founded, under circumstances envisaged in the AML Law;

suspicious financial transactions (activities) reasonably suspected to be associated with, related to or designated for terrorism financing or financing proliferation of weapons of mass destruction, and shall also inform relevant law enforcement authorities about such financial transactions and their participants.

7.2. Subject to the Local AML/CFT Laws, the Bank shall provide the following when requested by the FIU:

additional information which may be related to terrorism financing or financing proliferation of weapons of mass destruction, and information which may be related to suspension of financial transactions, freezing of assets associated with terrorism and financing thereof, proliferation of weapons of mass destruction and financing thereof;

additional information required by the FIU to fulfil requests received from a foreign authority;

information about tracking (monitoring) of financial transactions conducted by customers whose transactions have become subject to financial monitoring;

other information required by the FIU to perform its functions.

7.3. The Bank has developed and maintains channels enabling its employees to inform the Compliance Officer about unusual and/or suspicious customer transactions.

The Bank shall apply a risk-based approach to transaction monitoring, which includes automated and manual processes. Transaction monitoring shall be carried out in order to assess whether the customer's activities (their use of products and/or services and/or their general behavior) are consistent with the information received about the purpose and intended nature of the business relationship. As a part of the transaction monitoring, the Bank shall continue to investigate the activities considered as "unusual" or "suspicious" in relation to the activities declared by the customer when establishing the business relationship and/or obtained in the course of the customer service.

Automated transaction monitoring following a risk-based approach covers all business units, all customers, all market areas, and all products with appropriate scenarios. Manual transaction monitoring, i.e. the investigation and reporting of unusual activities to employees reporting about the money laundering, shall be achieved through training and operation of the reporting channels.

In order to inform the dedicated authority, the Bank provides for daily automated transaction monitoring proportional to the scope and complexity of financial transactions undertaken by the customers.

The term, manner and format of the Bank's notices provided to the FIU are defined in the Local AML/CFT Laws.

The notices are prepared and provided in electronic format using the National Bank's email software.

8. Bank staff training in AML/CFT

8.1. AML/CFT training is mandatory for all relevant Bank employees, is adapted to specific areas of the Bank's operations and assures an in-depth understanding by the employees of specific AML/CFT risks which they might face, and of their obligations related to such risks.

The Bank requires all employees to have an adequate level of awareness and ensures an appropriate level of awareness, in particular when the employees encounter something unusual related to the customer's behavior in their daily operations, they shall consider whether the unusual behavior may be related to AML/CFT issues and/or sanctions evasion.

8.2. The AML/CFT training designed for the staff is of high quality and relevance in the context of the AML/CFT risks and the Bank's commercial activities, and is consistent with effective obligations envisaged by the Local AML/CFT Laws, specifically the regulation on financial monitoring and internal controls. The AML/CFT training provides for:

continuous review by the Bank's employees of the Local AML/CFT Laws and international AML/CFT documents, with knowledge checks conducted in the form of regular tests and knowledge assessments;

mandatory review by the Bank's employees of the Bank's internal financial monitoring documents at the time of hire and in the event of changes in the documents;

practical training in the implementation of internal AML/CFT requirements;

creation of permanently available mechanisms for consultations on AML/CFT issues, empowering employees to notify about those policy or control aspects which they consider insufficiently clear/useful/efficient;

familiarization with the best practices regarding the detection of customers' financial transactions which may be associated with AML/CFT (typologies, schemes);

familiarization with CDD/EDD (enhanced due diligence) tools and techniques, including those designed to ascertain whether customers or persons acting on their behalf, their ultimate beneficiaries or beneficiaries belong to PEPs, to their connected or related parties; investigation of financial activities and conducting enhanced CDD of customers.

8.3. The Bank applies RBA to ensure that a wide range of employees can be trained through annual e-learning courses generated at the employee's workplace. Acknowledging the complexity of this area, the Bank also supports external certification and personal training for employees in key positions in this area.

Subject to Local AML/CFT Laws, the Bank implements measures to ensure that the Compliance Officer receives AML/CFT training.

8.4. The Bank continuously provides for the training of its staff in the identification of suspicious and threshold financial transactions, and for other financial monitoring actions by performing educational and practical work.

9. Establishing the relationshp with foreign financial or credit institutions

9.1. When establishing correspondent or similar relations with a foreign financial or lending institution (excluding financial institutions registered in the EU), the Bank applies, in addition to customer due diligence, enhanced due diligence measures in order to reinforce the monitoring and management activities and to reduce the risks.

Enhanced due diligence measures employed to verify a financial or lending institution include:

9.2. Collection of adequate information from reliable and independent sources to gain a fuller understanding of the nature of such financial or lending institution's operations and to determine its reputation and supervision quality, including whether the foreign financial institution was under an investigation in connection with money laundering or terrorism financing charges, or was subject to enforcement actions (sanctions) imposed by an authority exercising state regulation and supervision over the institution's activities whether a foreign financial institution has been the subject of an investigation into money laundering or terrorism financing, or the application of restrictions (sanctions) by an authority responsible for state regulation and supervision of its operations related to in the AML/CFT area.

9.3. Evaluation of the foreign financial or lending institution's AML/CFT activities.

9.4. Opening correspondent accounts for a foreign financial or lending institution and with foreign financial or lending institutions, and/or establishment of new correspondent relations with the approval of the Bank's Manager.

9.5. Recording the foreign financial or lending institution's obligations in the area of AML/CFT.

9.6. Gaining an assurance that a foreign financial or lending institution, whose accounts are directly used by third parties to conduct transactions in their own name, takes steps to conduct due diligence KYC (Know Your Customer) and CDD (Customer Due Diligence) of customers having direct access to the foreign financial or lending institution's accounts, and an assurance that the foreign financial or lending institution is able to provide at the Bank's request the relevant information obtained through CDD activities; submission of such requests.

9.7. Precluding the establishment or continuation of correspondent relations with a foreign financial or lending institution which allows its accounts to be used by shell banks, as based on the information obtained from reliable and independent sources.

9.8. The Bank does not enter into correspondent relations with foreign financial or lending institutions registered in the countries (territory), specified by Section 6 hereof (Sanctions Policy).

10. Final Provisions

10.1 This Policy shall become effective since it is approved by resolution of the Supervisory Board.

10.2 The Bank shall ensure the amendment of the Policy in accordance with the laws of Ukraine, as well as best international and domestic practices on AML/CFT. The amendments shall be approved by resolution of the Supervisory Board by restatement of the Policy.

10.3 In the event of amendment of the laws and/or the Articles of Association, the Policy provisions shall be effective to the extent, which is not in conflict with the laws of Ukraine and/or the Articles of Association.

10.4 The Bank shall introduce the procedures and rules aimed at implementation of the principles and provisions set forth herein.