SUMMARY OF THE RULES AND PROCEDURES FOR PREVENTION OF LEGALIZATION OF PROCEEDS FROM CRIME AND KNOW YOUR CUSTOMER RULES AND PROCEDURES

Organizational Structure

The in-house system for prevention of legalization of proceeds from crime or financing of terrorism (anti-money laundering and counter terrorist financing, hereinafter – AML/CTF) of Joint Stock Company the State Export-Import Bank of Ukraine (hereinafter – JSC Ukreximbank, the Bank) is headed by Director of the Financial Monitoring and Currency Supervision department (Money Laundering Reporting Officer). MLRO of the Bank is independent in his activity and reports to the Supervisory Board.

MLRO of the Bank heads, coordinates and controls the activity of the Financial Monitoring and Currency Supervision Department ("FMSCD") of the Bank and its structural units, in particular:

1. *Financial Monitoring Division*, covering, among other, the following lines of action:
   a. financial transactions' systemic analyses, monitoring and reporting,
   b. KYC programs and procedures.

2. *Currency Supervision Monitoring Division*, covering, among other, the following lines of action:
   a. customers' foreign economic activity controls,
   b. currency supervision monitoring.

Activity of the FMCSD and the AML/CFT compliance of the Bank is governed by the Ukrainian legislation in force, in particular by the Constitution and laws of Ukraine, including the Law of Ukraine On Banks and Banking, the Law of Ukraine On Prevention of and Counteraction to Legalization (Laundering) of Proceeds from Crime, Financing of Terrorism and the Financing of Proliferation of Weapons of Mass Destruction (hereinafter – the Law), Resolutions of the Verkhovna Rada of Ukraine (the Parliament), Decrees and Orders of the President of Ukraine, Decrees, Resolutions and Orders of the Cabinet of Ministers of Ukraine (the Government), regulations of the National Bank of Ukraine (the Central Bank and the regulator), and in particular Regulation on Financial Monitoring by Banks approved by Resolution of the Board of the National Bank of Ukraine No.65 dated 19.05.2020, regulations of the Ministry of Finance of Ukraine and of the State Financial Monitoring Service of Ukraine, the Statute (Articles of Association) of the JSC Ukreximbank, regulations of the Bank as well as by the recommendations of the Financial Action Task Force on Money

Laundering (hereinafter – FATF) and the Basel Committee on Banking Supervision.

The FMCSD ensures due functioning of the system of the Bank's compliance with the AML (financial monitoring) and currency laws and regulations in the following fields:

- prevention of and counteraction to legalization (laundering) of proceeds from crime, terrorism financing and financing of proliferation of weapons of mass destruction (AML/CTF/CFWMD);
- conduct of currency transactions and execution of currency controls;
- management of financial monitoring compliance risks;
- prevention of the risky activity, which is challenging the interests of depositors or other lenders of the Bank.

The Internal Audit Division ("IAD") on the risk-based approach shall audit the compliance of the activities of FMCSD and other units of the Bank as well as its regional branches with all legal requirements in the field of prevention of legalization of proceeds from crime/financing of terrorism (including the adequacy of steps taken by the Bank in respect of managing the risks of legalization of proceeds from crime/financing of terrorism) in accordance with the schedule approved. Based on such audit, the IAD shall issue its opinion and recommendations for the management of the Bank.

The IAD is subordinated to, controlled by and reports to the Supervisory Board of the JSC Ukreximbank.

Internal Policies and Procedures

In accordance with the Ukrainian law, the JSC Ukreximbank has developed and implemented its internal documents on financial monitoring:

- JSC Ukreximbank AML/CTF/CPF Risk Management Program,
- JSC Ukreximbank Rules for Customers' Financial Transactions/Activities Monitoring and Information Exchange with FIU,
- Customer Due Diligence Program of JSC Ukreximbank,
- the Program for Training and Professional Development of Employees in Prevention of Legalization of Proceeds from Crime/Financing of Terrorism,
- and others that define the procedure and conditions of the measures aimed at preventing the use of the Bank for the legalization (laundering) of proceeds from crime, terrorist financing and the financing of proliferation of weapons of mass destruction, including the order on UBO definition, the order on

PEP definition, and others.

Internal documents of the Bank on financial monitoring are aimed at:

- maintaining confidentiality of the fact of transmission of information on the customer's financial transaction to the authorized body (hereinafter – the State Financial Monitoring Service of Ukraine, or FIU);
- maintaining confidentiality of information on internal documents of the Bank on financial monitoring;
- maintaining confidentiality of information on accounts and deposits of the bank's customers, on the customers and their financial transactions, and other information constituting banking secrets;
- prevention of the bank employees' involvement in legalization of proceeds from crime/financing of terrorism.

The Rules and Programs are mandatory for all employees of the Bank involved in or ensuring: financial monitoring, identification, verification of the customers (customer representatives), customer analysis, identification (detection) and the assessment/reassessment of the risk of legalization of proceeds from crime/ financing of terrorism, monitoring of customers' risks, analysis of the risk of use of the Bank's services for legalization of proceeds from crime/financing of terrorism, etc., and entering into agreements, as well as for employees involved in conducting financial transactions via the Bank in accordance with their official duties.

The Bank's internal documents on financial monitoring shall be amended with regard to amendments to the Ukrainian law and events that may affect the risks of legalization of proceeds from crime/financing of terrorism. The compliance of such rules and procedures with the effective law shall be checked and reviewed on a regular basis.

The Rules and Programs include a description of the organizational structure of the in-house system for prevention of legalization of proceeds from crime/financing of terrorism and the financing of proliferation of weapons of mass destruction, as well as the basic principles of operation of AML compliance departments (tasks, functions, rights and duties) on prevention of legalization of proceeds from crime/financing of terrorism and the Procedures on:

- circulation and maintaining confidentiality of information on financial transactions, the fact of reporting to law enforcement authorities;
- analysis of financial transactions in order to identify the financial transactions that are subject to financial monitoring (mandatory, internal), can be connected with, related to or intended for terrorist financing or

proliferation of weapons of mass destruction, and if their participants or beneficiaries are on the list of persons involved in terrorist activity or are sanctioned persons.

When analyzing financial transactions of a customer, the Bank shall on the on-going basis implement a complex of risk-based measures enabling it to identify suspicious financial transactions of the customer.

Among others, the Bank checks the compliance/non-compliance of the financial transactions with the financial standing of the customer and the nature of its business; in particular, the Bank compares information obtained from the customer and the actual financial transactions in the accounts.

Within the time periods established by the Ukrainian Law and in accordance with the procedure established by the National Bank of Ukraine, the Bank shall report financial transactions reasonably identified as suspected to be intended for legalization of proceeds from crime or connected with, related to or intended for financing of terrorism or proliferation of weapons of mass destruction to the State Financial Monitoring Service of Ukraine;

- maintenance of financial transactions register, provision by the employees of the Bank to the compliance officer of the Bank with information on financial transactions and other information required to make a reasoned decision concerning entering information on financial transaction in financial transactions register and submission thereof to the State Financial Monitoring Service of Ukraine;
- satisfaction of requests, decisions (orders) of the State Financial Monitoring Service of Ukraine in the cases stipulated by the Law;
- suspension and renewal of financial transactions;
- keeping of official documents and other documents (including reports prepared by the compliance officer of the Bank in accordance with the requirements of law, internal regulations on suspension (renewal) of financial transactions) and information on financial monitoring issues. According to the requirements of the applicable law of Ukraine the Bank shall keep official documents and other documents (including electronic documents created by the Bank) related to identification of persons (customers, customer representatives) as well as persons whose financial transactions were denied by the Bank, customer analysis, clarification of customer information and copies thereof, as well as all documents related to business relations (financial transaction) of the customer (including results of any analysis conducted during customer verification or in-depth customer identification) – for at least five years after the financial transaction

completion, termination of business relations with the customer; all required information on financial transactions (sufficient to monitor the transaction) – at least five years after the transaction completion, closing of an account, termination of business relations.

Customer Due Diligence Program (related to customer identification, verification and analysis) shall include distribution of duties and designation of the Bank' divisions and/or employees to be responsible for customer (customer's representatives) identification, verification, customer financial condition assessment and clarification/additional clarification of information on the customer and/or persons acting on behalf of the customer is conducted as well as the Procedures on:

- identification, verification of customer (customer's representative), person by or on behalf of whom the financial transaction is conducted;
- obtaining of information and/or documents for identification of the ultimate beneficial owner (controller) of the customer, beneficiaries under financial transaction, including a list of relevant procedures specifying requested information and/or documents;
- risk-based in-depth identification, clarification/additional clarification of customer information (enhanced due diligence of a customer), including the nature of its activity and financial condition, customer reputation assessment (customer reputation assessment shall cover the following issues: duration of business relations with the Bank; customer track record; services used by the customer; economic activity; country of customer origin; financial problems; reputation of counterparts, etc.);
- detection of affiliation of the customer or a person acting on its behalf to politically exposed persons (hereinafter – PEPs), to persons associated or related to PEPs (related persons are persons with whom family members of domestic, foreign PEPs and persons performing political functions in international organizations have business or personal relations, as well as legal entities, the ultimate beneficial owners (controllers) of which are such persons or their family members or persons with whom such persons have business or personal relations) in the process of their identification, verification and servicing; identification of steps taken by the Bank in accordance with the risk-based approach to identify the sources of funds of such persons (assets, rights to such assets, etc.) on the basis of documents provided by them and/or information from other sources, if such information is public (open), granting of permission for establishment/maintenance/renewal of business relations with such persons;

- study of the customer's financial activity, including procedures of the on-going risk-based analysis of the customer's financial transactions in order to detect those financial transactions, which are inconsistent with the customer's financial standing (with the customer's financial condition assessment) and/or with the nature of the customer's economic activity, which have no or unclear economic expediency (sense), or which can otherwise expose the Bank to (or involve the Bank into conducting) the risky activity, which is challenging the interests of depositors or other lenders of the Bank, or to the actions provisioned by the Criminal Code of Ukraine. In the course of analysis of the customer's financial transactions, the Bank's officers take all measures as may be appropriate to come to the conclusion on consistence/inconsistence of such financial transactions with the customer's financial standing and the nature of their economic activity as well as to make reassessment of the customer's risk;
- conduct of verification of the customer's identification data against possible matches with the data of sanctioned persons designated by the National Security and Defense Council of Ukraine, the UNSC, the US OFAC, the US FinCEN, the EU, FATF and other relevant authorities;
- conduct of early automated checking of financial transactions with software tools in order to detect and suspend the financial transaction before it is conducted in favour or by order of the Bank's customer, where a party to or a beneficiary of the transaction is included into the lists of persons related to terrorism activity, or the list of persons to whom international sanctions apply;
- maintenance of electronic customer profile, which ensures timeliness, completeness and correspondence of the information entered into the electronic questionnaire of the customer with the data contained in the file of the customer;
- refusal of establishment (maintenance) of business (contractual) relations (including through termination of contractual relations) or performance of financial transaction.

The Bank shall perform identification, verification of the customer (person, customer representative) and take steps prior to establishment of business (contractual) relations executed in writing (entering into agreements), opening of an account, performance of one-time financial transactions in the significant amount as well as clarification/additional clarification of customer information in the process of customer analysis.

According to the legal requirements, the Bank shall perform identification and

verification of the customers/persons (customer representatives), in particular:

- customers which establish business relations with the Bank;
- customers (other than banks registered in Ukraine), which open accounts with the Bank;
- customers, which carry out transactions that are subject to the financial monitoring;
- customers (persons) in case of suspicion that financial transactions carried out by them may be related to financing of terrorism or financing of proliferation of weapons of mass destruction;
- customers, performing financial transactions with virtual assets in the amount equal to or exceeding 30,000 Hryvnias;
- customers, which carry out financial transactions with cash without opening an account for the amount exceeding 400,000 Hryvnias or its equivalent, including in foreign currency, banking metals, other assets;
- customers from which the Bank shall raise funds under the terms and conditions of a subordinated debt;
- customers, which enter with the Bank into loan agreements, safe custody agreements or safe deposit box rent agreements;
- persons (other than banks registered in Ukraine) with which the Bank as a professional securities market participant shall enter into agreements to carry out professional activity in the securities market (stock market). From the date of such agreement such a person shall be the customer of the Bank;
- persons authorized to act on behalf of the said customers/persons (customer representatives).

If the Bank has doubts concerning accuracy and completeness of the customer information, it shall perform in-depth identification (enhanced due diligence) that includes obtaining of additional information (data) about the customer (including its representatives and/or beneficiaries) concerning identification analysis of the customer (including customer owners) under financial transactions performed, data, copies of documents on financial transactions in order to confirm or defy the suspicions concerning legalization (laundering) of proceeds from crime or financing of terrorism that arose in the process of customer servicing.

The Bank may in the process of verification of information submitted by the customer use independent sources of information, including official websites of the authorized government bodies; mass-media; information obtained from the public authorities, civil registrars, other banks; other legal entities or other sources, if such

information is public (open).

The Bank shall perform the assessment of the customer's financial standing based on the analysis of economic and social indicators, including quantitative and qualitative factors that may in some way affect identification of correspondence of transactions carried out by the customer with its financial capacity.

The Bank shall refuse to establish (maintain) business relations (including via termination of business relations) or to perform financial transaction in case where the identification and/or verification of the customer (including data verification enabling to identify the ultimate beneficial owners (controllers)) is impossible or in case of suspicion that the person is not acting on its own behalf; if identification and/or verification of the customer (in-depth verification of the customer) revealed that the provided information was incorrect or false to mislead the Bank.

The Bank shall be obliged to refuse to establish (maintain) business relations/refuse the customer to open an account (render services), including by terminating business relations, closing the account/refuse to conduct a financial transaction in the following cases:

- if the identification and/or verification of the customer, as well as the establishment of data enabling the establishment of the ultimate beneficial owners, is impossible, or if the Bank has doubts that the person is acting on his/her own behalf;
- establishment of an unacceptably high risk for the customer or the customer's failure to provide the documents or information necessary for the customer's due diligence;
- inaccurate information submission by the customer or his/her representative to the Bank or submission of information for the purpose of misleading the Bank;
- detection, in accordance with the procedure established by the relevant subject of state financial monitoring, that a bank or other financial institution with which correspondent relations are established is a shell bank and/or maintains correspondent relations with a shell bank;
- if it is impossible to identify the person on whose behalf or in whose interests the financial transaction is being conducted, and to establish its ultimate beneficial owner or beneficiary under the financial transaction.

The Bank has the right to refuse to carry out a suspicious financial transaction.

The Bank shall not open and not maintain anonymous (numbered) accounts; not establish correspondent relations with shell banks, and with non-resident banks and

other financial institutions maintaining correspondent relations with shell banks; not enter into contractual relations (not carry out foreign exchange transactions, transactions with banking metals, cash transactions) for legal entities or individuals, in case of suspicion that the legal entity or individual is not acting on its own behalf, or if they are included in the list of persons related to terrorism activity, or are sanctioned persons or entities, and in other cases stipulated by the Law.

AML/CTF/CPF Risk Management Program includes Procedures for customer classification and criteria (indicators) for assessing the customer's risk given the nature of financial transactions and their frequency, criteria (indicators) for assessing the risk of use of the Bank's services for legalization of proceeds from crime/terrorism financing, customer risk monitoring and analysis, identifying appropriate precautions to prevent, limit and/or reduce to the acceptable level of the identified risks of legalization of proceeds from crime/terrorism financing.

The structure of the Bank's money laundering / terrorism financing risk management system consists of the following levels:

1st line of defense, which includes business units, support units of the Bank, which are involved in the processes of establishing business relations with customers / customer service, and which directly initiate, carry out (support) the processes of applying measures for customer due diligence, accept the AML/FT risks in the course of their activities and are responsible for the current management of these risks, including for non-fulfillment of duties and/or inactivity in the field of AML/CFT in accordance with their official duties and/or orders of the Bank's management;

2nd line of defense, which at the level of the Financial Monitoring Division and the Bank's MLRO ensures the organization of the intra-bank AML/CFT system and the Bank's primary financial monitoring, in accordance with the requirements of the AML/CFT legislation and the Bank's internal documents on financial monitoring;

3rd line of defense, which includes the Bank's internal audit unit that carries out an independent assessment of the effectiveness of the 1st and 2nd lines of defense and a general assessment of the intra-bank AML/CFT system functioning (the Bank's conduct of primary financial monitoring).

The customer risk is determined at all stages of the customer servicing with consideration of the following **main components of risk/risk criteria groups**:

- customer type,
- geography,

- type of service (product) provided,
- service (product) delivery channel,
- reputation.

During customer service, the following **criteria groups of financial transactions' suspicion signs** are applied:

- Indicators related to the activity or behaviour of the customer,
- Indicators related to the customer's financial transactions,
- Indicators for different types of products (services).

Some examples of the risks criteria/indicators considered by the Bank:

if the customer is a non-profit organization; a PEP, or a PEP-related or associated person; a business entity organizing lotteries and gambling, including casinos, electronic (virtual) casinos; a provider of currency exchange and/or money transfer services (other than banks and postal services operators); a foreign company, control over and management of which is performed on the basis of the power of attorney; an entity whose owner of significant share, ultimate beneficiary owner (controller), officers are foreign or domestic PEP(s), or a PEP-related persons; a trust, a trust fund, or an entity with a complicated ownership structure; a non-resident joint stock company issuing bearers share; a foreign financial institution seeking establishment of correspondent relations (other than financial institutions registered in the EU or FATF member countries); a political party; an entity connected with arms production or sale;

the customer fails to submit information and data envisaged by Ukrainian legislation or internal regulations of the Bank; has complicated (multilevel, with non-residents involved) ownership structure, which complicates the process of identification of its true owner or beneficiary; there are doubts as to the reliability or completeness of the information provided; the customer performs financial transactions that do not correspond with their financial condition and/or nature of business;

the customer is included into the list by the State Financial Monitoring Service of Ukraine as a person related to terrorism activity or a person to whom international sanctions were applied; the customer is included into the list of persons to whom sanctions were applied (if sanctions' types and terms envisage that financial operations of such persons shall be suspended or prohibited); if special measures (sanctions) were applied by the National Security and Defense Council of Ukraine to the customer's related persons;

significant increase of the customer's daily account balance, which is regularly withdrawn in cash over the bank's counter by the customer or their representative; regular cash withdrawal of funds from the customer's banking account(s) credited with third party(-ies) transfers, except for salaries, scholarship and retirement allowance, social (welfare) payments; attempted exceeding by the customer of cash settlements limits established by the Law; transfer of funds abroad as an advance payment for the imports, if the country of residence of the beneficiary and the country of the beneficiary's bank are different; type of products, works (services) that are the subject matter of a foreign economic agreement is not typical for the ordinary business of the customer; regular receipt/provision/return by the customer of financial aid, loan, debt facility or other borrowings; the customer performs financial transactions that have complicated or unusual nature, or it is a set of interconnected financial transactions that have no obvious economic substance or obvious legal purpose; the customer conducts repeated financial transactions whose nature gives reasons to suspect that their purpose is to avoid mandatory financial monitoring or identification (verification) envisaged by the Law;

the country of stay (residence) or the registration of the customer or of the agency used by the customer to transfer (receive) assets is known from reliable sources as identified among the jurisdictions (territories) that do not comply with the recommendations of international, intergovernmental organizations involved in prevention and counteraction to legalization (laundering) of proceeds from crime, or terrorism financing, or proliferation of weapons of mass destruction financing; is included by the Cabinet of Ministers of Ukraine (the Government) into the list of offshore zones; is supporting international terrorism, or is being subject to international sanctions, embargos or other restrictive measures under the UNSC resolutions and/or Ukrainian legislation in force; the customer who/whose UBO is a citizen of the state that carries out armed aggression against Ukraine ("aggressor state"), and/or is a resident of/was created and registered in accordance with the legislation of the aggressor state and/or a person whose place of permanent residence (stay, registration) is the aggressor state; the customer whose management structure and/or management bodies/manager include/is a citizen of the aggressor state and/or a person whose place of permanent residence (stay, registration) is the aggressor state; the customer who has business relations with a citizen of the aggressor state and/or a person whose place of permanent residence (stay, registration) is the aggressor state, or who has business relations with a legal entity created and registered in accordance with the legislation of the aggressor state, and other.

The Bank uses **four-level ranking to classify the levels of risk** of the Bank's involvement into legalization (laundering) of proceeds from crime or terrorism financing. Based on the selected criteria, the following **risk categorie**s are assigned to customers:

- unacceptably high risk (high risk subcategory);
- high risk;
- average risk;
- low risk.

The Bank uses the risk assessment scoring method that envisages establishment of risk level indicators based on the sum of points assigned for each risk criterion. The risk level indicator may range from zero (inclusively) and higher.

By the results of customers' risk monitoring and services risk analysis and assessment, AML department may review the points assigned for each criterion.

In the course of assignment/change of the customer's risk level, if the customer falls under at least one of the risk criteria, such a customer's risk level may not be determined as "low". If the customer's risk is determined as average and tends to grow (including reaching a high level of risk), the customer incurs an increased risk of transactions related to legalization (laundering) of proceeds from crime or terrorism financing.

The risk level assigned to the customer is subject to the on-going review (changes) following the results of the Bank's monitoring of the customer's risk, with account of risk-related financial transactions performed by them that are subject to financial monitoring, and their frequency.

The Bank fills the customer questionnaire with information (data), reliability of which is confirmed by know-your-customer documents and other documents available to the Bank.

The questionnaire is an internal electronic document of the Bank, which contains all the information obtained by the Bank through identification, know your customer procedures, specified data regarding the customer's identification and KYC procedures, in-depth customer analysis (enhanced due diligence), as well as the Bank's opinion on assessment of the customer's risk, with indication of dates of such assessments.

The Bank shall ensure availability (should a hard copy of the questionnaire be required) of all the data in the electronic questionnaire with mandatory indication of information related to identification, in-depth customer analysis (enhanced due diligence) and analysis of the customer's financial operations, as well as changes of the customer's risk level, dates of questionnaire amendments regarding

identification and analysis.

The Bank shall be obliged to assign the category of ***high risk*** to the customer based on the sum of points determined in accordance with the Banks' risk program and/or in case of establishing the relevant risk criteria, for example, if (the list below is not exhaustive):

- negative character is assigned to the customer's reputation;
- discrepancy between the financial transaction(s) and the customer's financial condition and/or nature of their activity is identified;
- determination of compliance/incompliance of the financial transaction(s) to the customer's financial condition is impossible;
- determination of the nature and purpose of the financial transaction(s) following the results of all measures taken by the Bank's officers in compliance with legislative requirements in force (in particular, by requesting additional documents and data related to the financial transaction with mandatory recording of the date of receipt of such documents and data) is impossible;
- there are doubts in credibility or fullness of the information provided by the customer, including based on the results of in-depth analysis of such a customer;
- it is established that the customer is a national, foreign politically exposed person or a person performing political functions in international organizations (PEPs) or a their close or associated person;
- the customer is a person whose accounts were credited with funds illegally debited from other persons' accounts;
- the customer's domicile (residency, registration) is the country where recommendations of FATF and other international organizations whose task is prevention of legalization of proceeds from crime/terrorism financing are not applied or applied to an insufficient extent;
- The customer, their UBO is a citizen and/or resident/was created and registered in accordance with the legislation of the aggressor state and/or a person whose place of permanent residence (stay, registration) is the aggressor state;
- the customer is a foreign financial institution [other than financial institutions registered in the European Union member countries, FATF member countries, except for states that carry out armed aggression against Ukraine in the sense specified in Article 1 of the Law of Ukraine "On the

Defense of Ukraine"] with which correspondent relations are being established;

- the country is on the list of Jurisdictions (territories) that do not comply or do not properly comply with the recommendations of international, intergovernmental organizations involved in prevention and counteraction to legalization (laundering) of proceeds from crime, or terrorism financing, or proliferation of weapons of mass destruction financing;
- the country supports terrorism, is subject to international sanctions, embargos or other restrictive measures under the UNSC resolutions and/or Ukrainian legislation in force;
- the customer is from the country (territory) on the list of the offshore areas approved by the Cabinet of Ministers of Ukraine;
- the customer is on the list of persons connected with terroristic activity, or persons subject to international sanctions;
- other cases stipulated by the internal policy.

The Bank shall assign the category of ***unacceptably high risk*** to the customer, if:

- unacceptable character is assigned to the customer's reputation, based on the following:
    - the customer/their UBO/persons who have the right to manage the customer's accounts are on the wanted list,
    - there is information available information in official and/or public sources about the customer, their UBO or manager regarding their involvement in terrorist activities and/or involvement in collaborative activities,
    - there is information available information in official sources about the customer, their UBO or the customer's manager regarding their involvement in actions aimed at violent change or overthrow of the constitutional order or at the seizure of state power,
    - there is information available in official sources about the customer, their UBO or the customer's manager regarding their involvement in actions threatening the territorial integrity and inviolability of Ukraine,
    - there is information available in official sources about the customer, their UBO or the customer's manager regarding their involvement in treason,

- there is information available in official sources about the customer, their UBO or the customer's manager regarding their assistance to the aggressor state,
- there is information available in official sources about the customer, their UBO or the customer's manager regarding their involvement in the falsification of financial documents and reporting of a financial organization, concealment of the insolvency of a financial institution,
- there is information available about the lost/invalid identification document of the customer/their officers and/or about the registration of a legal entity based on stolen, lost documents or documents of persons who have died or do not exist;

- the customer is included in the list of terrorists, the customer is a representative of the persons included in the list of terrorists, the customer is directly or indirectly owned or the customer's UBO is the persons included in the list of terrorists,
- the customer does not provide the information required by the legislation of Ukraine and/or the internal regulatory documents of the Bank and/or provides inaccurate information or provides information with the purpose of misleading the Bank,
- customers (persons), regarding whom the Bank, based on the results of studying the customer's activities, has well-founded suspicions that they have carried out AML/CFT operations, other crimes,
- if it is impossible to fulfill the obligations defined by the legislation on AML/CFT or to minimize the identified risks related to the customer or financial transaction,
- it was detected in accordance with the procedure established by the NBU that a bank or other financial institution with which correspondent relations are established is a shell bank and/or maintains correspondent relations with a shell bank,
- if suspicions that the customer is a shell company (carrying out fictitious activities) have been confirmed based on a set of criteria.
- Other risk criteria that may indicate an Unacceptably high level of risk.

To ensure functioning of the system for management of risks of legalization of proceeds from crime/financing of terrorism the Bank shall perform *in-depth analysis (**enhanced due diligence**) and take additional steps* regarding customers to which the category of high-risk was assigned, including but not limited to the following:

1. Regarding the foreign financial institution with which correspondent relations are being established:

- ensure collection of information about its reputation, as well as whether the foreign financial institution was subject to enforcement measures (sanctions) by an authority responsible for state regulation and supervision of its activity in the field of prevention of and counteraction to legalization (laundering) of proceeds from crime and financing of terrorism;
- determine what steps are taken by the financial institution to prevent and counteract to legalization (laundering) of proceeds from crime, financing of terrorism, and financing of proliferation of weapons of mass destruction, including the financial institution's KYC policy and procedures;
- based on obtained information, assess the sufficiency and effectiveness of steps taken by the financial institution to counteract to legalization (laundering) of proceeds from crime, financing of terrorism and financing of proliferation of weapons of mass destruction;
- open correspondent accounts for the foreign financial institution and with foreign financial institutions subject to the authorization by the Chairman of the Management Board;
- take other measures stipulated by the internal policy.

2. Regarding national and foreign politically exposed persons and persons performing political functions in international organizations, their associated or related persons (related persons are persons with whom family members of national and foreign politically exposed persons and persons performing political functions in international organizations have business or personal relations, as well as legal entities whose ultimate beneficial owners (controllers) are such politically exposed persons or their family members or persons with whom such politically exposed persons have business or personal relations):

- determine if the customer or the person acting on its behalf pertains to the mentioned category of customers, when performing identification, verification, and while rendering services to them, and if they are ultimate beneficial owners (controllers) or managers of legal entities, and establish business relations with such customers subject to the authorization by the Bank's Top Manager;
- prior to or during establishment of business relations, take steps to determine sources of such persons' funds, assets and wealth based on the documents obtained from them and/or information from other sources, if such information is public, that confirm sources of their assets, rights to

such assets, etc.;

- perform primary financial monitoring of financial transactions;
- update the customer information based on the risk level assigned;
- take other measures stipulated by the internal policy.

Management of risks of legalization of proceeds from crime/terrorism financing shall be direct responsibility of the Bank's compliance officer.

The Program for Training and Professional Development of Employees in Prevention of Legalization of Proceeds from Crime/Financing of Terrorism envisages direct participation of every employee (within their competence) in the process of prevention of legalization of proceeds from crime/terrorism financing, and such training/advance training shall be carried out at least once a year via on-site, part-time, and remote educational and practical work.

Training shall include studying of international and national regulations, recommendations on counteraction to legalization of proceeds from crime of the Basel Committee on Banking Supervision, the Bank's internal regulations, rules, and procedures, as well as practical training.

Advance training shall include studying state-of-the-art expertise regarding detection of the customer financial transactions that may be connected with legalization of proceeds from crime/terrorism financing (typologies, schemes), as well as familiarization with customer studying means and techniques, including determination whether the customer or the person acting on its behalf, its ultimate beneficial owners (controllers), beneficiaries pertain to politically exposed persons, persons associated or related to politically exposed persons, studying the customer financial activity and in-depth analysis of the customer.

The Bank's compliance officer shall undergo training and advance training pursuant to the procedure established by the Cabinet of Ministers of Ukraine (the Government).

The Bank's employees may improve their skills through other forms of training (topical workshops, practical workshops, conference workshops, round table meetings, including self-education, etc.).