

Затверджено:
Генеральний директор

ТОВ «ЕКСПАНДІА»

Сергій Сергієнко



Політика щодо боротьби з легалізацією доходів, отриманих злочинним шляхом (відмиванням грошей)

П-ГО.00-004

1. Вступ

Компанія CBRE Україна («Компанія») розробила Політику щодо боротьби з легалізацією доходів, отриманих злочинним шляхом (надалі – боротьба з відмиванням грошей – «БВГ»), що викладена у цьому документі («Політика»). Ця політика спрямована на усунення ризиків відмивання грошей, що пов'язані з веденням бізнесу Компанії, її партнерів та/або афілійованих осіб, клієнтів, підрядників та працівників.

2. Сфера застосування

Ця Політика застосовується до усіх департаментів/працівників Компанії, з особливою увагою до працівників, що надають посередницькі послуги під час здійснення операцій з купівлі-продажу нерухомого майна, а також консультативні послуги, що пов'язані з купівлею-продажем нерухомого майна.

3. Ідентифікація ризиків, пов'язаних з відмиванням грошей

- Визначення відмивання грошей

Легалізація (відмивання) доходів, отриманих незаконним/злочинним шляхом, включає будь-які дії, пов'язані зі здійсненням фінансових транзакцій чи правочинів, де залучені доходи, отримані

злочинним шляхом, а також вчинення дій, спрямованих на приховування незаконного походження таких доходів або прав на такі доходи, їх джерел, розміщення, переміщення, зміни їх форми, а також отримання злочинних доходів, володіння чи користування ними.

Відмивання грошей через угоди з нерухомим майном дозволяє інтегрувати доходи, отримані незаконним шляхом, у легальну економіку завдяки безпечному інвестуванню. Таким чином злочинці отримують змогу користуватись майном та доходами, замаскувавши походження грошей, використаних у якості оплати.

- Приклади відмивання грошей через операції з нерухомістю

Використання готівки. Купівля нерухомості за готівку – тривіальний, але ефективний метод відмивання грошей.

Занижена або завищена оцінка вартості – різниця у вартості компенсується таємними платежами готівкою.

Треті сторони – Злочинці купують нерухомість через третіх осіб – законних власників, що не мають кримінального минулого.

Оренда - Майно надається в оренду орендарю, який отримує незаконні кошти для здійснення платежів.

Підставні компанії, трасти та інші подібні структури – Придбання нерухомості через підставну компанію дозволяє зберегти в таємниці ім'я власника.

- Навіщо потрібна Політика

Політика має на меті надати Компанії змогу дотримуватись вимог щодо звітності та інших застосовних вимог законодавства України щодо БВГ та інших норм і правил щодо боротьби з шахрайством та тероризмом.

- Застосовне законодавство

Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» від 06.12.2019 р., № 361-IX;

Підзаконні акти, керівництва та рекомендації, розроблені Службою фінансового моніторингу України.

4. Основні обов'язки Компанії у сфері БВГ (первинного фінансового моніторингу):

призначення чи звільнення відповідального працівника;

призначення особи, яка тимчасово буде виконувати обов'язки відповідального працівника у разі його відсутності;

забезпечувати відповідно до вимог, встановлених відповідним суб'єктом державного фінансового моніторингу, належну організацію та проведення первинного фінансового моніторингу, що належним чином надасть можливість виявляти порогові та підозрілі фінансові операції (діяльність) незалежно від рівня ризику ділових відносин з клієнтом (проведення фінансових операцій без встановлення ділових відносин) та повідомляти про них спеціально уповноважений орган;

запобігати використанню послуг та продуктів суб'єкта первинного фінансового моніторингу для проведення клієнтами фінансових операцій з протиправною метою;

забезпечувати функціонування належної системи управління ризиками, застосування у своїй діяльності ризик-орієнтовного підходу та вжиття належних заходів з метою мінімізації ризиків;

здійснювати належну перевірку нових клієнтів, а також існуючих клієнтів;

забезпечувати реєстрацію фінансових операцій, що підлягають фінансовому моніторингу, зокрема з використанням засобів автоматизації;

сприяти в межах законодавства працівникам спеціально уповноваженого органу у проведенні аналізу фінансових операцій;

подавати на запит спеціально уповноваженого органу, що вчинений в межах його повноважень, додаткову інформацію, що може бути пов'язана з фінансуванням тероризму чи фінансуванням розповсюдження зброї масового знищення;

вживати заходів щодо запобігання розголошенню (зокрема особам, стосовно фінансових операцій яких проводиться перевірка) інформації, що подається спеціально уповноваженому органу, та іншої інформації з питань фінансового моніторингу (у тому числі про факт подання такої інформації або факт отримання запиту, рішення чи доручення від спеціально уповноваженого органу та їх виконання), крім випадків, визначених чинним законодавством;

документувати заходи, вжиті з метою виконання вимог законодавства у сфері запобігання та протидії відмиванню грошей;

вживати на постійній основі заходів з підготовки персоналу з метою належного виконання вимог цього Закону, зокрема шляхом проведення освітньої та практичної роботи;

здійснювати управління ризиками, пов'язаними із запровадженням чи використанням нових та існуючих інформаційних продуктів, ділової практики або технологій, у тому числі таких, що забезпечують проведення фінансових операцій без безпосереднього контакту з клієнтом;

встановлювати для працівників процедури щодо повідомлення керівника суб'єкта первинного фінансового моніторингу та/або відповідального працівника про порушення вимог законодавства у сфері запобігання та протидії, у тому числі без зазначення авторства (анонімно), із забезпеченням відповідних засобів;

не допускати формування свого статутного капіталу за рахунок коштів, джерела походження яких неможливо підтвердити;

інші обов'язки Компанії, що впливають з закону про БВГ.

5. Відповідальний працівник (Compliance Officer)

Відповідальний працівник призначається за посадою на рівні керівництва суб'єкта первинного фінансового моніторингу. Відповідальний працівник повинен мати бездоганну ділову репутацію та відповідати кваліфікаційним вимогам, встановленим Державною службою фінансового моніторингу.

До повноважень відповідального працівника належать:

1) забезпечення повідомлення спеціально уповноваженого органу про фінансові операції, що підлягають фінансовому моніторингу;

2) забезпечення повідомлення спеціально уповноваженого органу про розбіжності між відомостями про кінцевих бенефіціарних власників клієнта, що містяться в Єдиному державному реєстрі юридичних осіб, фізичних осіб - підприємців та громадських формувань, та інформацією про кінцевих бенефіціарних власників, отриманою суб'єктом первинного фінансового моніторингу в результаті здійснення належної перевірки клієнта;

3) проведення перевірок діяльності будь-якого підрозділу суб'єкта первинного фінансового моніторингу та його працівників щодо виконання ними внутрішніх документів з питань фінансового моніторингу;

4) право доступу до всіх приміщень, документів, інформації, баз даних, технічних засобів електронних комунікацій, архівів суб'єкта первинного фінансового моніторингу;

5) залучення працівників суб'єкта первинного фінансового моніторингу до проведення первинного фінансового моніторингу та перевірок з цих питань;

6) організація розроблення, подання для затвердження, забезпечення постійного оновлення, а також контроль за виконанням внутрішніх документів з питань фінансового моніторингу;

7) одержання пояснень з питань проведення фінансового моніторингу від працівників суб'єкта первинного фінансового моніторингу незалежно від займаних посад;

8) сприяння проведенню уповноваженими представниками суб'єктів державного фінансового моніторингу, що відповідно до цього Закону виконують функції державного регулювання та нагляду за відповідними суб'єктами первинного фінансового моніторингу, перевірок діяльності суб'єкта первинного фінансового моніторингу щодо дотримання законодавства у сфері запобігання та протидії;

9) прийняття рішення про подання інформації з питань фінансового моніторингу на запити спеціально уповноваженого органу та відповідних правоохоронних органів;

10) виконання інших функцій відповідно до законодавства та внутрішніх документів з питань фінансового моніторингу.

6. Звітування до Державної служби фінансового моніторингу України

Компанія, через Відповідального працівника, повідомляє спеціально уповноважений орган про:

а) порогові фінансові операції, що відповідають ознакам, визначеним абзацами другим та третім частини першої статті 20 Закону про БВГ, - протягом п'яти робочих днів з дня їх проведення (спроби проведення);

б) порогові фінансові операції, що відповідають ознакам, визначеним абзацами четвертим та п'ятим частини першої статті 20 Закону про БВГ, - не пізніше п'ятого робочого дня місяця, наступного за місяцем, в якому фінансові операції були здійснені;

в) підозрілі фінансові операції (діяльність) або спроби їх проведення незалежно від суми, на яку вони(а) проводяться, - негайно після виникнення підозри або достатніх підстав для підозри, а також надавати обґрунтовані висновки, копії документів та іншу інформацію, на основі яких сформовано підозру, та додаткову інформацію на запити спеціально уповноваженого органу;

г) про розбіжності між відомостями про кінцевих бенефіціарних власників клієнта, які містяться в Єдиному державному реєстрі юридичних осіб, фізичних осіб - підприємців та громадських формувань, та інформацією про кінцевих бенефіціарних власників, отриманою суб'єктом первинного фінансового моніторингу в результаті здійснення належної перевірки клієнта, - не пізніше десятого робочого дня місяця, наступного за місяцем, в якому були виявлені розбіжності.

7. Перевірка за санкційними переліками

Перед початком встановлення ділових відносин чи відкриттям аккаунту для нового клієнта, Компанія перевіряє, чи не включена така особа до будь-якого переліку санкцій чи обмежень. Одним з таких переліків є Спеціальний чорний список осіб, що публікується Управлінням США з контролю за іноземними активами (OFAC) - [the US Specially Designated Nationals List \(SDN\)](#).

Компанія забезпечує дотримання процедури перевірки клієнтів за вказаними переліками, а також обізнаність із останніми змінами до них.

Від клієнтів вимагатиметься підписання господарських договорів, що містять стандартне «санкційне застереження», розроблене Компанією.

Відповідальними з боку Компанії є: Юридичний відділ, Менеджер з закупівель, Відповідальний працівник.

8. Застосування ризик-орієнтованого підходу

Компанія зобов'язана у своїй діяльності застосовувати ризик-орієнтований підхід, враховуючи відповідні критерії ризику, зокрема, пов'язані з його клієнтами, географічним розташуванням держави реєстрації клієнта або установи, через яку він здійснює передачу (отримання) активів, видом товарів та послуг, що клієнт отримує від суб'єкта первинного фінансового моніторингу, способом надання (отримання) послуг.

Ризик-орієнтований підхід – означає визначення (виявлення), оцінка (переоцінка) та розуміння ризиків легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму та/або фінансування розповсюдження зброї масового знищення, а також вжиття відповідних заходів щодо управління ризиками у спосіб та в обсязі, що забезпечують мінімізацію таких ризиків залежно від їх рівня.

Ризик-орієнтований підхід має бути пропорційний характеру та масштабу діяльності Компанії.

Застосування ризик-орієнтованого підходу здійснюється в порядку, визначеному внутрішніми документами з питань фінансового моніторингу суб'єкта первинного фінансового моніторингу, з урахуванням рекомендацій відповідних суб'єктів державного фінансового моніторингу, які згідно із цим Законом виконують функції державного регулювання і нагляду за такими суб'єктами первинного фінансового моніторингу.

Компанія зобов'язана здійснювати оцінку/переоцінку ризиків, у тому числі притаманних її діяльності, документувати їх результати, а також підтримувати в актуальному стані інформацію щодо оцінки ризиків, притаманних його діяльності (ризик-профіль суб'єкта первинного фінансового моніторингу), та ризику своїх клієнтів таким чином, щоб бути здатним продемонструвати своє розуміння ризиків, що становлять для нього такі клієнти (ризик-профіль клієнтів).

Критерії ризику визначаються Державною службою фінансового моніторингу України. Керівництво з ризик-орієнтованого підходу розроблено на основі стандартів міжурядової Групи з розробки фінансових заходів боротьби з відмиванням грошей (FATF); текст Керівництва доступний українською мовою та буде доведений до відома усіх заінтересованих осіб Компанії.

9. Здійснення аудиту (перевірки) контрагентів (KYC)

Цей крок стосується заходів, вжитих у рамках CDD для тих, хто визначений як бенефіціарний власник, вищого керівництва, політично відомих осіб (PEP) тощо. Компанія також повинна вказати основу своєї системи оцінки ризиків, як вона визначає, чи вимагає спрощеної належної перевірки, належної перевірки клієнта або посиленої належної перевірки.

Високий ризик – означає результат оцінки ризиків Компанією, що ґрунтується на результатах аналізу сукупності визначених критеріїв, передбачених законодавством та внутрішніми документами Компанії, що свідчить про високу ймовірність використання Компанії для цілей легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму та/або фінансування розповсюдження зброї масового знищення.

Компанія зобов'язана встановити високий ризик ділових відносин (фінансової операції без встановлення ділових відносин), зокрема стосовно таких клієнтів:

клієнтів, місцем проживання (перебування, реєстрації) яких є держава (юрисдикція), що не виконує чи неналежним чином виконує рекомендації міжнародних, міжурядових організацій, задіяних у сфері боротьби з легалізацією (відмиванням) доходів, одержаних злочинним шляхом, або фінансуванням тероризму чи фінансуванням розповсюдження зброї масового знищення.

Перелік держав (юрисдикцій), що не виконують чи неналежним чином виконують рекомендації міжнародних, міжурядових організацій, задіяних у сфері боротьби з легалізацією

(відмиванням) доходів, одержаних злочинним шляхом, або фінансуванням тероризму чи фінансуванням розповсюдження зброї масового знищення, формується в порядку, визначеному Кабінетом Міністрів України на основі висновків міжнародних, міжурядових організацій, задіяних у сфері боротьби з легалізацією (відмиванням) доходів, одержаних злочинним шляхом, або фінансуванням тероризму чи фінансуванням розповсюдження зброї масового знищення, та оприлюднюється на офіційному веб-сайті спеціально уповноваженого органу;

клієнтів, включених до переліку осіб, клієнтів, які є представниками осіб, включених до переліку осіб, клієнтів, якими прямо або опосередковано володіють або кінцевими бенефіціарними власниками яких є особи, включені до переліку осіб;

іноземних фінансових установ (крім фінансових установ, зареєстрованих у державах - членах Європейського Союзу, державах - членах Групи з розробки фінансових заходів боротьби з відмиванням грошей (FATF), крім держав, що здійснюють збройну агресію проти України у значенні, наведеному у статті 1 Закону України "Про оборону України"), з якими встановлюються кореспондентські відносини;

іноземних публічних діячів, членів їх сімей та осіб, пов'язаних з такими політично значущими особами, а також клієнтів, кінцевими бенефіціарними власниками яких є зазначені особи;

клієнтів, стосовно яких (кінцевих бенефіціарних власників яких) застосовані спеціальні економічні та інші обмежувальні заходи (санкції) відповідно до статті 5 Закону України "Про санкції";

клієнтів, місцем проживання (перебування, реєстрації) яких є держава, віднесена Кабінетом Міністрів України до переліку офшорних зон.

Компанія вживає відповідних запобіжних заходів, спрямованих на здійснення посиленних заходів належної перевірки до встановлення ділових відносин з особами або компаніями таких держав; повідомлення спеціально уповноваженого органу про фінансові операції з клієнтами відповідних держав; попередження клієнтів про те, що операції з фізичними або юридичними особами, трастами або іншими подібними правовими утвореннями у відповідних державах можуть містити ризик легалізації (відмивання) доходів, одержаних злочинним шляхом, або фінансування тероризму чи фінансування розповсюдження зброї масового знищення.

Approved:
General Director

EXPANDIA LLC

Sergiy Sergiyenko



Anti -Money Laundering Policy

P-GO.00-004

1. Introduction

CBRE Ukraine has developed the Anti-Money Laundering (AML) Policy described in the present document (the Policy). The Policy is intended for elimination of money laundering risks described herein with regard to business activities of CBRE Ukraine, its partners and/or affiliates, clients, contractors and employees.

2. Field of Application

The Policy shall apply to all departments/employees of CBRE Ukraine, with a special focus on employees engaged in providing intermediary services in real estate sale and purchase transactions as well as colleagues providing consulting services related to sale and purchase of real estate.

3. Identification of the Risks Related to Money Laundering

- Definition of the ML

Legalization (laundering) of proceeds from crime shall cover any actions related to execution of financial transaction or deed with proceeds from crime, as well as commission of actions aimed at concealing or disguising the illicit origin of such proceeds or their ownership, rights to such proceeds, sources of their

origin, location, movement, change in their form (transformation), as well as acquisition, possession or use of proceeds from crime.

Money laundering through real estate transactions integrates illicit funds into the legal economy while providing a safe investment. It allows criminals to enjoy assets and derived funds, having camouflaged the origin of the money used for payment.

- Examples of Money Laundering through Real Estate

Cash deposits. Using cash to buy a property is an unsophisticated, but often effective, method of money laundering.

Under-and over-valuation -the difference in property value is settled in secret cash payments.

Third-party purchases -Criminals buy real estate using a third party (often someone with no criminal record) as the legal owner.

Leasing -A property is rented to a tenant, who is provided with illicit funds to cover the payments

Shells, trusts and other company structures. -Purchasing property through a shell company allows the name of the owner of the property to be kept secret.

- Why the Policy is Necessary

The Policy is intended to enable the company to comply with and report on the applicable requirements of the local Anti-Money Laundering legislation of Ukraine, and other anti-fraud/ anti-terrorism regulations.

- Applicable Legislation

The Law of Ukraine On Preventing and Counteracting to Legalization (Laundering) of the Proceeds from Crime, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction dd. December 6, 2019 No. 361-IX;

Regulatory acts, handbooks and recommendations developed by the State Financial Monitoring Service of Ukraine.

4. Basic AML Responsibilities of the Company in the Field of AML:

appoint a compliance officer; appointment of a person who will temporarily perform the duties of a compliance officer in his/her absence;

ensure according to local requirements proper organization and implementation of initial financial monitoring, which will allow to properly detect threshold and suspicious financial transactions (activities) irrespective of the level of risk of business relations with a customer (conducting financial transactions without establishing business relations) and to report them to the specially authorized body (the State Financial Monitoring Service of Ukraine);

prevent the use of services and products of the Company for the conduct of financial transactions by customers for unlawful purpose;

ensure the functioning of the appropriate risk management system, application a risk-oriented approach in its activities and to take appropriate measures to mitigate risks;

conduct due diligence of new customers as well as existing customers;

ensure registration of financial transactions that are subject to financial monitoring, in particular with the use of automation tools;

assist, within the scope allowed by the law, the personnel of the specially authorized body in the analysis of financial transactions;

submit upon a request of the specially authorized body made within its powers: a) additional information that may be related to financing of terrorism or financing of proliferation of weapons of mass destruction;

take measures to prevent disclosure (in particular, to persons whose financial transactions are being verified) of information submitted to the specially authorized body and other information on financial monitoring (including on the fact of submission of such information or the fact of receipt of a request, a decision or an order from the specially authorized body and execution thereof);

document the measures taken to comply with the requirements of the AML legislation;

train personnel on a regular basis for the purpose of proper compliance with the requirements of the Law, in particular through educational and practical work;

manage risks associated with the introduction or use of new and existing information products, business practices or technologies, including those that ensure conducting financial transactions without direct contact with a customer;

establish procedures for the personnel regarding informing head of the Company and/or a compliance officer of the AML requirements violation, including without indication of authorship (anonymously), with the provision of appropriate means;

prevent the formation of its authorized capital (for credit unions - share, reserve and additional capital) at the expense of funds, the sources of origin of which can't be confirmed

other obligations of the Company pursuant to the ML Law of Ukraine.

5. The Compliance Officer

A compliance officer shall be appointed at the managerial level of the Company. The compliance officer shall have an impeccable business reputation and meet qualification requirements set by the Company, who pursuant to local legislation shall perform functions of state regulation and supervision over the Company.

The authority of the compliance officer shall include:

- 1) ensuring reporting a specially authorized body on financial transactions subject to financial monitoring;
- 2) ensuring reporting a specially authorized body about discrepancies between information on ultimate beneficial owners of a customer contained in the Unified State Register of Legal Entities, Private Entrepreneurs and Public Formations and information about ultimate beneficial owners received by the Company as a result of customer due diligence;
- 3) conducting the audits of activities of any unit of the Company and its officers concerning their compliance with internal documents on financial monitoring;
- 4) the right for access to all premises, documents, information, databases, means of telecommunications, archives of the Company;
- 5) involving any Company officers in the initial financial monitoring and inspections on these matters;
- 6) organization of development, submission for approval, ensuring constant updating, as well as monitoring of compliance with internal documents on financial monitoring;
- 7) obtaining explanations on the matters of conducting financial monitoring from the Company officers, regardless of the positions occupied;
- 8) providing assistance to the authorized representatives of state financial monitoring entities, which pursuant to this Law shall perform functions of state regulation and supervision over the relevant reporting entities, in conducting inspections of the Company activities concerning compliance with the AML legislation;
- 9) making a decision on submission of information on financial monitoring at requests of a specially authorized body and the relevant law enforcement agencies;
- 10) performing other functions pursuant to the legislation and internal documents on financial monitoring.

6. Reporting to the State Financial Monitoring Service of Ukraine

The Company through the Compliance Officer shall notify the specially authorized body of the following:

- a) threshold financial transactions which meet the features defined in the Law – within five business days from the day of their conduct (attempted conduct);
- b) threshold financial transactions which meet the features defined in the Law – no later than the fifth business day of the month following the month in which the financial transactions were conducted;
- c) suspicious financial transactions (activities) or attempts to conduct them, regardless of the amount for which they (it) are (is) conducted – immediately after the occurrence of a suspicion or sufficient grounds for a suspicion, and also to provide justified conclusions, copies of documents and other information on the basis of which suspicions have been formed and additional information on the requests of the specially authorized body;
- d) on discrepancies between information about ultimate beneficial owners of a customer contained in the Unified State Register of Legal Entities, Private entrepreneurs and Public Organizations and information about ultimate beneficial owners received by a reporting entity as a result of customer due diligence – no later than the tenth business day of the month following the month in which discrepancies were detected.

7. Screening Across Sanctions List

Before entering a business relationship or opening an account for a client, the Company must verify that the person they are working with is not on any sanction or blocklist. One example of such is the US Specially Designated Nationals List (SDN).

The company must ensure compliance with the procedure for checking their clients through these lists and establish their awareness of the latest changes.

Clients shall be required to sign commercial agreements containing a standard “Sanctions Clause” developed by the Company.

Responsible departments/officers of the Company shall be: Legal; Sourcing; Compliance Officer.

8. Application of the Risk-Oriented Approach

The Company is obliged, in its activities, to apply a risk-oriented approach, taking into consideration the relevant risk criteria, in particular, those related to its customers, geographical location of the state of customer registration or institution through which it transfers (receives) assets, type of goods and services that the customer receives from a reporting entity, the way of providing (receiving) services.

The risk-oriented approach shall mean identification (revealing), assessment (reassessment) and understanding of the risks of legalization (laundering) of proceeds from crime and/or terrorism financing or financing of weapons of mass destruction, as well as taking appropriate measures to manage risks in the manner and within the scope that ensure minimization of such risks depending on their level.

A risk-oriented approach shall be proportional to the nature and scale of the Company’s activities.

A risk-oriented approach shall be applied in accordance with the procedure established by the internal documents on financial monitoring of a reporting entity, taking into account the recommendations of the relevant state financial monitoring entities, which, in accordance with this Law, perform functions of state regulation and supervision of such reporting entities.

The Company is obliged to assess/reassess risks, including those inherent in its activities, document their findings as well as keep updated the information on the assessment of risks inherent in its activities (risk profile of a reporting entity) and the risk of its customers in such a way as to be able to demonstrate its understanding of the risks posed to it by such customers (risk profile of a customer).

The risk criteria are determined by the State Financial Monitoring Service of Ukraine. The Handbook on Risk-Oriented Approach has been developed based on FATF standards, is available in the Ukrainian language and shall be communicated to all persons concerned within the Company.

9. Performing Customer Due Diligence (KYC)

This step is about the measures taken as a part of CDD for those identified as beneficial owners, senior management, politically exposed persons (PEP), etc. The company should also specify the basis of its risk rating system, how it determines whether the case requires simplified due diligence, customer due diligence, or enhanced due diligence.

Here, it would be necessary to add when a customer triggers adverse media or sanctions list checks, be subject to ongoing monitoring.

High risk shall mean the result of risk assessment by the Company, which is based on the analysis results of the aggregate of defined criteria, provided for by the legislation and internal documents of the Company that testifies a high probability of the use of the Company for the purpose of legalization (laundering) of proceeds from crime, financing of terrorism and/or financing proliferation of weapons of mass destruction.

The Company is obliged to establish a high risk of business relations (financial transaction without establishing business relations), in particular with respect to the following customers:

- customers, whose place of residence (stay, registration) is a country (jurisdiction), which do not or do not properly comply with the recommendations of international, intergovernmental organizations engaged in AML;
- a list of countries (jurisdictions) that do not or do not properly comply with the recommendations of international, intergovernmental organizations involved in AML is formed in the manner defined by the Cabinet of Ministers of Ukraine, based on the findings of international, intergovernmental organizations involved in AML/CFT and is published on the specially authorized body official website;
- customers included in the list of persons, customers who are representatives of persons included in the list, customers directly or indirectly owned, or the ultimate beneficial owners of which are persons included in the list;
- foreign financial institutions (except for financial institutions registered in the European Union Member Countries, Member Countries of the Financial Action Task Force (FATF), except for the countries conducting armed aggression against Ukraine in the meaning referred to in Article 1 of the Law of Ukraine “On Defence of Ukraine”), with which correspondent relations are established;
- international politically exposed persons, their family members and persons related to such politically significant persons, as well as customers, whose ultimate beneficial owners are mentioned persons;
- customers regarding which (ultimate beneficial owners of which) special economic and other restrictive measures (sanctions) are applied in accordance with Article 5 of the Law of Ukraine “On Sanctions”;
- customers, whose place of residence (stay, registration) is a country included by the Cabinet of Ministers of Ukraine in the list of offshore zones.

The Company shall take appropriate preventive measures aimed at: adopting enhanced due diligence measures prior to establishing business relations with persons or companies of such countries; notifying a specially authorized body of financial transactions with customers of the relevant countries; warning of customers that transactions with individuals or legal entities, trusts or other similar legal arrangements in the relevant countries may contain risk of laundering of proceeds from crime or financing of terrorism or financing of proliferation of weapons of mass destruction.

