Додаток 20
до Публічної пропозиції АТ «КРИСТАЛБАНК» на укладення договору комплексного банківського обслуговування фізичних осіб

Умови і правила надання послуг з використанням мобільного застосунку «CrystalBank»

Ці Умови і правила надання послуг з використанням мобільного застосунку «CrystalBank» (надалі - Умови) є невід'ємною частиною Публічної пропозиції АТ «КРИСТАЛБАНК» на укладення договору комплексного банківського обслуговування фізичних осіб (далі – Публічна пропозиція, Договір), що укладений між АКЦІОНЕРНИМ ТОВАРИСТВОМ «КРИСТАЛБАНК» (надалі – Банк) та фізичною особою, що акцептувала умови Публічної пропозиції АТ «КРИСТАЛБАНК» на укладення договору комплексного банківського обслуговування фізичних осіб (надалі –Клієнт), в подальшому разом – Сторони, а окремо – Сторона.

Ці Умови регламентують загальні правила надання послуг з використанням мобільного застосунку «CrystalBank», визначають загальний порядок і умови отримання доступу, здійснення платіжних операцій та дистанційної комунікації з Клієнтом в межах наявних рахунків за допомогою мобільного застосунку «CrystalBank».

1. ВИЗНАЧЕННЯ ТЕРМІНІВ.

автентифікаційні дані – набір даних, що використовуються Банком для ідентифікації і автентифікації під час користування Клієнтом мобільного застосунку «CrystalBank»;

автентифікація – процедура, що дає змогу Банку установити та підтвердити особу Клієнта та/або належність Клієнту певного платіжного інструменту, наявність у нього підстав для використання конкретного платіжного інструменту, у тому числі шляхом перевірки індивідуальної облікової інформації Клієнта. Автентифікація Клієнта, що обслуговується через мобільний застосунок «CrystalBank», здійснюється за зареєстрованим (фінансовим) номером, але з метою додаткового захисту під час звернення Клієнта до Банку, Банк має право також запитати у Клієнта іншу інформацію, вказану в Заяві-договорі про приєднання до Публічної пропозиції.

Для автентифікації у мобільному застосунку «CrystalBank» Банк використовує посилену автентифікацію;

авторизаційні дані – це сукупність інформації (наприклад, логін і пароль), яка використовується для підтвердження особистості Клієнта (аутентифікація) та надання йому дозволів на доступ до мобільного застосунку «CrystalBank» або виконання дій у мобільному застосунку «CrystalBank»;

активація – процес, за допомогою якого вразливі платіжні дані, пристрої або програмне забезпечення для цілей автентифікації або посиленої автентифікації стають повністю функціональними і готовими до використання Клієнтом, який має/повинен мати законне право на їх використання;

Банк – АКЦІОНЕРНЕ ТОВАРИСТВО «КРИСТАЛБАНК», код за ЄДРПОУ 39544699, місцезнаходження: вул. Кудрявський узвіз, 2, м. Київ, 04053, в складі структурних та відокремлених підрозділів, надавач платіжних послуг;

біометричні дані – сукупність автоматизованих методів і засобів ідентифікації людини (Клієнта), заснованих на її фізіологічній або поведінковій характеристиці. В мобільному застосунку можуть використовуватись наступні технології біометричних даних:

- Touch ID (та подібні) – сканер відбитків пальця(-ів);
  Face ID (та подібні) – сканер обличчя особи;

віддалена ідентифікація та верифікація – встановлення ділових відносин з Клієнтом без його фізичної присутності в Банку;

геопозиціонування телефону – процес визначення географічних координат телефону;

«Дія» (МЗ Дія) – державний мобільний застосунок та вебпортал в Україні, який забезпечує доступ до цифрових державних послуг та документів, який розроблений Міністерством цифрової трансформації України. Застосунок дає змогу зберігати в смартфоні документи фізичних осіб, а саме: водійське посвідчення, паспорт громадянина України, паспорт громадянина України для виїзду за кордон, інші документи, а також передавати їхні копії при отриманні банківських та інших послуг;

електронний документ – це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа, та створений, переданий, збережений, перетворений у візуальну форму електронними засобами;

канал комунікації – канал, що забезпечує Банку передавання клієнту інформації про його послуги, включно із засобами масової інформації (періодичні друковані видання, інтернет, блоги, онлайн-платформи), соціальними мережами, платіжними, включно з мобільними застосунками, каналами дистанційного електронного обслуговування [телефон, месенджер (Viber), банкомат, мережа Інтернет та інші засоби, пов'язані з електронною комунікаційною мережею], крім власного вебсайту Банку;

кваліфікований електронний підпис «Дія.Підпис» (Дія.Підпис) - кваліфікований електронний підпис, який створюється за допомогою мобільного застосунку Єдиного державного вебпорталу електронних послуг згідно з вимогами законодавства. Дія.Підпис є КЕП Клієнта;

Клієнт– фізична особа, що користується мобільним застосунком «CrystalBank» або має намір ним скористатися;

мобільний застосунок «CrystalBank» (далі – мобільний застосунок) – система дистанційного обслуговування клієнтів, призначена для роботи на смартфонах та інших мобільних електронних пристроях (за наявності інтрнету), та представляє собою «Інтернет-банкінг CrystalBank (Мобільний інтерфейс)» з можливістю відкриття рахунків Клієнтам в т.ч. з ЕПЗ, визначених у цій Публічній пропозиції, без відвідування відділення Банку, управління доступними банківськими продуктами, здійснення платіжних операцій за рахунками на підставі електронних платіжних інструкцій, отримання інформації;

одноразовий код – унікальний ідентифікатор (цифровий код), що генерується Банком на підставі параметрів банківської (в т. ч. платіжної) операції та надсилається Банком Клієнту за допомогою SMS-повідомлення на мобільний номер, та використовується Клієнтом з метою підтвердження його особи під час виконання банківських (в т. ч. платіжних) операцій з використанням реквізитів ЕПЗ. Одноразовий код є дійсним тільки для одного сеансу автентифікації протягом певного проміжку часу;

офіційний вебсайт Банку (далі – сайт Банку) – https://crystalbank.com.ua/;

пароль для входу (тут і далі – «пароль») – це таємне слово або набір латинських літер верхнього та нижнього регістру, цифр та спеціальних символів, призначені для підтвердження особи або повноважень, які відомі лише Клієнту та використовується ним з метою підтвердження входу клієнта до мобільного застосунку «CrystalBank. Довжина пароля складає від 6 до 15 символів. Замість пароля може використовуватися відбиток пальця Touch ID або цифровий образ обличчя Face ID чи код доступу за наявності технічної можливості мобільного пристрою;

посилена автентифікація – процедура автентифікації Клієнта через мобільний застосунок «CrystalBank», яка передбачає використання двох чи більше сукупностей даних, що належать до таких різних категорій:

- знань (володіння інформацією (даними), що відома лише Клієнту, наприклад: пароль);
- володінь (застосування матеріального предмета, яким володіє лише Клієнта, наприклад мобільний телефон з фінансовим номером);
- притаманність (перевірка біометричних даних або інших властивостей (рис, характеристик), притаманних лише Клієнту, що відрізняють його від інших клієнтів, наприклад відбиток пальця Touch ID або цифровий образ обличчя Face ID);

рахунок – будь-який рахунок(и) Клієнта, що відкритий(і) у Банку на умовах відповідного

укладеного договору між Клієнтом та Банком;

регламентні роботи – тимчасові роботи, що пов'язані з технічним обслуговуванням мобільного застосунку «CrystalBank» або банківських операційних систем, під час проведення яких Банком встановлюються обмеження доступу до мобільного застосунку «CrystalBank» та обробки електронних документів;

сервіси мобільних платежів – система мобільних платежів, яка дозволяє здійснювати розрахунки за товари/послуги/роботи за допомогою мобільного пристрою. Оплата відбувається через відповідний додаток з використанням технології NFC;

SMS-повідомлення – технологія, що дозволяє відправляти та отримувати текстові електронні повідомлення за допомогою послуг оператора мобільного зв'язку, наявності відповідного засобу мобільного зв'язку (зокрема, мобільного телефону), або за допомогою будь-яких інших мобільних та WEB додатків, визначених договором між Клієнтом та Банком як канал комунікації (зокрема, але не виключно Viber та інші) або за допомогою Push-повідомлень;

фінансовий номер – номер мобільного телефону Клієнта українських операторів мобільного зв'язку, який зазначений в Заяві-договорі про приєднання або інших заявах, які надані у відділені Банку чи за допомогою мобільного застосунку «CrystalBank» та підтверджений Клієнтом як номер телефону, за допомогою якого може проводитися дистанційна автентифікація Клієнта, укладення правочинів, обслуговування, підтвердження фінансових операцій, повідомлення розміру простроченої заборгованості, неустойки та інших платежів;

цифровий електронний платіжний засіб (цифрова картка) – електронний платіжний засіб, що існує без фізичного носія у електронному вигляді, тобто у формі набору даних, які ідентифікують держателя ЕПЗ і відображаються за допомогою дистанційних каналів обслуговування;

CRS (Common Standard on Reporting and Due Diligence for Financial Account Information) або Загальний стандарт звітності та належної перевірки інформації про фінансові рахунки (далі - Загальний стандарт звітності CRS) – це міжнародний стандарт, схвалений Радою ОЕСР 15 липня 2014 року, що вимагає від країн, які його імплементують, здійснювати збір інформації від фінансових установ про фінансові рахунки власників рахунків. АТ «КРИСТАЛБАНК» є фінансовим агентом у зв'язку із приєднанням України до Багатосторонньої угоди CRS та набранням 28.04.2023 чинності Закону України від 20.03.2023 №2970-IX «Про внесення змін до Податкового кодексу України та законодавчих актів України щодо імплементації міжнародного стандарту автоматичного обміну інформацією про фінансові рахунки». Банк зобов'язаний здійснювати заходи належної комплексної перевірки фінансових рахунків клієнтів та серед власників рахунків (у певних випадках і серед їх контролюючих осіб) виявляти осіб, які є податковими резидентами інших підзвітних юрисдикцій-партнерів з обміну інформацією;

Touch ID – сканер відбитків пальців, датчик дозволяє Клієнтам проводити розблокування пристроїв, а також підтверджувати свої дії online/offline в мобільному застосунку. Використовується для біометричної авторизації;

Face ID – сканер об'ємно-просторової форми обличчя людини, сканер дозволяє Клієнтам проводити розблокування пристроїв, а також підтверджувати дії online/offline в мобільному застосунку. Використовується для біометричної авторизації;

FATCA (Foreign Account Tax Compliance Act) — нормативний акт Міністерства фінансів США (Department of Treasury) і Податкового управління США (Internal Revenue Service, IRS) для протидії ухиленню від сплати податків в США. В українське законодавство вимоги FATCA імплементовані угодою №840_005-17 від 07.02.2017 між Урядом України та Урядом Сполучених Штатів Америки для поліпшення виконання податкових правил й застосування положень Закону США «Про податкові вимоги до іноземних рахунків» (FATCA), який набув чинності 1 липня 2014 року.

PUSH-повідомлення – повідомлення Банку, що надсилаються з метою надання та/або у зв'язку із наданням Банком банківських та/або інших послуг передбачених цими Умовами та/або іншими договорами укладеними між Банком та Клієнтом, які відображаються як спливаюче вікно на екрані мобільного пристрою Клієнта, на якому встановлено мобільний застосунок «CrystalBank».

2. ЗАГАЛЬНІ ПОЛОЖЕННЯ

2.1. Дистанційне обслуговування за допомогою мобільного застосунку «CrystalBank» дозволяє без відвідування Клієнтом Банку здійснювати Банку дистанційну ідентифікацію та верифікацію клієнта-фізичної особи, відкриття рахунку, укладати договори банківського рахунку в електронній формі, здійснювати операції за рахунками, а також оплату послуг/товарів/робіт та перекази коштів, інші банківські операції, інші операції/дії, що передбачені Публічною пропозицією.

2.2. Операції Клієнта за рахунками та інші окремі дії щодо рахунків виконуються за допомогою мобільного застосунку в межах та з урахуванням діючих тарифів Банку, параметрів продукту, в рамках якого було відкрито рахунок, порядку та режиму функціонування такого рахунку, які передбачені чинним законодавством України та Договором, невід'ємною частиною якого є ці Умови.

2.3. Доступ до мобільного застосунку надається на безстроковій основі до моменту настання обставин, які відповідно до цих Умов призводять до припинення Договору.

2.4. Банк не гарантує конфіденційність і безпеку електронної передачі даних через сторонні підключення, які не перебувають під контролем Банку. Конфіденційність та безпека передачі даних забезпечуються відповідно до регламентів компаній, які надають послуги сервісу мобільних платежів.

2.5. Будь-які дії Клієнта з мобільним застосунком потребують доступу до мережі Internet, крім дії з оплати товарів/послуг/робіт за допомогою зареєстрованих електронних платіжних засобів в гаманці.

2.6. Доступ до мережі Internet, а також до інших технічних засобів та програмного забезпечення, що є необхідними для користування мобільним застосунком, не є предметом цих Умов і забезпечується Клієнтом самостійно і за власні кошти. Технічні та програмні засоби, за допомогою яких Клієнт здійснює доступ до мережі Internet, повинні відповідати вимогам, наведеним в Умовах, а їх справність, безпечність та належне функціонування в повному обсязі покладаються на Клієнта.

2.7. Правочини, пов'язані із наданням банківських (фінансових/платіжних) послуг через мобільний застосунок «CrystalBank», передбачених Договором, можуть вчинятися Сторонами з використанням електронного підпису, а саме: КЕП Банку та/або ЦВП Клієнта/одноразового коду/Дія.Підпис. При цьому Дія.Підпис використовується виключно для віддаленої ідентифікації Клієнта шляхом шерингу документів Клієнта через МЗ Дія; одноразовий пароль/ЦВП є аналогами власноручного підпису за домовленістю Сторін відповідно до ст. 207 Цивільного кодексу України, прирівнюються до особистого підпису Клієнта, а накладення ЦВП Клієнта/одноразового коду/КЕП Банку має рівнозначні юридичні наслідки із власноручним підписом Клієнта та/або Банку на документах на паперових носіях. ЦВП Клієнта/одноразовий код використовується Клієнтом як електронний підпис для підтвердження операції з Банком, що є окремим реквізитом документа/операції/дії, який надає документу/операції/дії юридичної сили, дає змогу підтвердити цілісність підписаних даних Клієнта та факт того, що документ в електронній формі підписав Клієнт. Дія.Підпис/ЦВП Клієнта/одноразовий код не можуть бути визнаними недійсними через їх електронну форму.

2.8. Під час здійснення операцій після активації мобільного застосунку – виконання в програмних комплексах маніпуляцій, спрямованих на успішне завершення операції/дії/документа (за необхідності), прирівнюється до електронного підпису Клієнта. Згоду Клієнта може бути підтверджено: a) документом в електронному вигляді з застосуванням одноразового коду; b) введенням ПІН-коду, паролів доступу до мобільного застосунку, використання відбитка пальця Клієнта за допомогою технології TouchID або за допомогою використання технології розпізнавання обличчя FaceID.

2.9. Для операцій/дій/документів, для яких в мобільному застосунку не вимагається підтвердження одноразового коду, операції/дії/документи можуть підтверджуватися без введення одноразового коду, лише натисканням Клієнта на відповідну кнопку на сторінці мобільного застосунку. Натискання на відповідну кнопку засвідчує бажання Клієнта вчинити відповідну дію та всі правочини, операції, угоди, документи/ініціативи, дії. Даний спосіб

підтвердження не може бути визнаним недійсним через його електронну форму, або через те, що він не має статусу електронного цифрового підпису. Після натискання на відповідну кнопку підтвердження Клієнт одноосібно несе відповідальність за зміст такої операції/дії/документа.
2.10. Всі банківські операції, угоди, інші документи/ініціативи, здійснені в електронному вигляді, є електронними документами і прирівнюються до таких, що укладені із додержанням письмової форми, і не можуть бути оскаржені через їх електронну форму.
2.11. Надання Клієнту доступу до мобільного застосунку не позбавляє Клієнта можливості отримання банківських послуг у відділеннях Банку.
2.12. Клієнт здійснює користування мобільним застосунком відповідно до законодавства України, нормативно-правових актів Національного банку України, Договору та цих Умов.
2.13. Банком розроблена та впроваджена сукупність правил та норм, відповідно до яких здійснюється користування мобільним застосунком «CrystalBank». Посилання на інструкцію розміщене на офіційному Інтернет-сайті Банку https://crystalbank.com.ua/ua/mobile-app/.

3. ПОРЯДОК НАДАННЯ ДОСТУПУ ДО МОБІЛЬНОГО ЗАСТОСУНКУ «CrystalBank»

3.1. Клієнт здійснює завантаження МЗ Дія та проходить процедуру реєстрації в цьому додатку.
3.2. Клієнт здійснює генерування в МЗ Дія кваліфікованого електронного підпису Дія.Підпис, який накладається Клієнтом на хеш цифрових ідентифікаційних документів в момент його шерингу з МЗ Дія до мобільного застосунку «CrystalBank». Порядок Клієнта за посиланням: https://ca.diia.gov.ua/faq_diia_id.
3.3. Для отримання доступу до мобільного застосунку «CrystalBank» для пристроїв з операційною системою iOS/Android, Клієнт завантажує мобільний застосунок «CrystalBank» через відповідні сервіси (AppStore або Google Play), які підтримує операційна система мобільного пристрою, після чого проводиться процедура реєстрації (створення облікового запису у мобільному застосунку), а саме:

- вводиться фінансовий номер у відповідній графі мобільного застосунку;
- проводиться автентифікація за допомогою одноразового коду, що надходить Клієнту на вказаний фінансовий номер;
- здійснюються заходи належної перевірки, зокрема: віддалена ідентифікація та верифікація за допомогою МЗ Дія. Клієнт надає Банку е-документи (паспорт громадянина України у вигляді ID-картки або закордонний паспорт), фото Клієнта зроблене методом розпізнавання реальності особи (Liveness detection);
- надання згоди на обробку персональних даних;
- проведення анкетування Клієнта;
- здійснення автентифікації Клієнта за допомогою одноразового коду, що надійшов на його фінансовий номер;
- створення Клієнтом пароля, який буде використовуватися для посиленої автентифікації у мобільному застосунку.

Після реєстрації Клієнта та перевірки пакета документів, мобільний застосунок активується, в результаті чого Клієнт отримує доступ до функцій та послуг Банку за допомогою мобільного застосунку.
3.4. Під час анкетування Клієнт зазначає наступну інформацію:

- електронну адресу;
- фактичне місце проживання;
- ознаку співпадіння фактичної адреси з адресою реєстрації;
- приналежність до податкових резидентів США (FATCA);
- приналежність до податкових резидентів юрисдикції іншої ніж Україна або США (CRS);
- володіння часткою в іноземній юридичній особі (КІК);
- приналежність до політично значущих осіб, членів їх сімей або до пов’язаних з ними осіб;
- наявність у Клієнта або пов’язаною з ним особою зв’язку із державою, що здійснює збройну агресію проти України (російська федерація /республіка білорусь);

- відомості про освіту;
- відомості про соціальний статус;
- відомості про працевлаштування (місце роботи, посада);
- джерела та обсяги надходження коштів та інших цінностей на рахунки;
- максимальну суму надходжень на рахунки за місяць;
- послуги (продукти), якими користується Клієнт/планує користуватися у Банку;
- чи зареєстрований Клієнт як фізична особа підприємець або як особа, що здійснює незалежну професійну діяльність;
- слово пароль.

3.5. Реєстрація дозволяється за умови дотримання наступних вимог:
- зареєстрована адреса електронної пошти має бути унікальна. Це означає, що жоден Клієнт раніше не використовував такі дані під час реєстрації;
- зареєстрований номер телефону Клієнта є фінансовим та має бути унікальним. Це означає, що жоден клієнт раніше не використовував такі дані під час реєстрації;
- активація мобільного застосунку здійснюється шляхом посиленої автентифікації, це може здійснюватися за допомогою пароля, TouchID або FaceID..

3.6. Допускається три невдалих спроби автентифікації поспіль, після трьох невдалих спроб автентифікації поспіль проводиться автоматичне блокування Клієнта у мобільному застосунку. Розблокування здійснюється на підставі особистого звернення Клієнта за телефонними номерами контакт-центру Банку, розміщеними на сайті Банку.

3.7. Максимальний час без активності Клієнта після проходження посиленої автентифікації не перевищує 5 (п’яти) хвилин, після чого доступ до мобільного застосунку закривається.

4. ЗАГАЛЬНІ УМОВИ НАДАННЯ БАНКІВСЬКИХ ПОСЛУГ ЗА ДОПОМОГОЮ МОБІЛЬНОГО ЗАСТОСУНКУ «CrystalBank»

4.1. Відповідно до цих Умов за допомогою мобільного застосунку Клієнт може здійснювати такі операції (в т.ч. платіжні):
- оплата послуг (комунальних, поповнення мобільного тощо) шляхом використання сервісу агрегатора послуг Portmone;
- перегляд загальної інформації за рахунками: балансу рахунків, історії операцій тощо);
- перекази коштів між власними рахунками Клієнта, що відкриті в Банку, включаючи: погашення заборгованості за кредитами, включаючи овердрафти; переказ коштів на вкладні (депозитні) рахунки (поповнення) – виключно у разі, якщо такі операції передбачено відповідною Заявою-договором про приєднання, укладеною між Банком та Клієнтом; переказ коштів з вкладних (депозитних) рахунків Клієнта на рахунки Клієнта (повернення вкладу) – виключно у разі, якщо такі операції передбачено відповідною Заявою-договором про приєднання, укладеною між Банком та Клієнтом; переказ коштів з рахунку Клієнта на рахунки інших Клієнтів Банку – фізичних осіб, відкриті в Банку;
- переказ коштів в національній валюті з рахунку Клієнта на його рахунки та рахунки фізичних або юридичних осіб, відкриті в Банку та/або інших банках України, можливість використання сканування QR-коду;
- переказ коштів на ЕПЗ інших Клієнтів Банку
- переказ коштів на ЕПЗ клієнтів інших банків;
- відображення реквізитів для поповнення поточного рахунку через інші банки;
- формування виписок за рахунками Клієнта;
- встановлення/зміна лімітів операцій, що можуть бути здійснені з використанням платіжної картки;
- відкриття поточного рахунку, замовлення нового ЕПЗ;
- відкриття депозиту онлайн;
- купівля, продаж безготівкової іноземної валюти (обмін валюти);
- перегляд курсів валют, встановлених Банком: для платіжних операцій з використанням ЕПЗ, для операцій купівлі/продажу іноземної валюти у відділеннях Банку та офіційного курсу гривні щодо іноземних валют НБУ;

- отримання PUSH-повідомлення про рух коштів ініційованих ЕПЗ;
- дебетове списання коштів з рахунку за згодою Клієнта (договірне списання).

4.2. З метою зменшення ризиків проведення помилкових операцій, а також для протидії шахрайським операціям, Банк встановлює ліміти на операції, які здійснюються з використанням ЕПЗ, (далі за текстом – ліміти), з якими Клієнт може ознайомитись на сайті Банку.

4.3. Банк не виконує операції/дії у разі, якщо здійснення переказу на визначену Клієнтом суму перевищують встановлені ліміти.

4.4. Керуючись положеннями статті 207 Цивільного кодексу України, Банк під час надання Клієнту виписок, довідок, квитанцій може використовувати факсимільне відтворення підпису посадової особи Банку та печатки Банку за допомогою засобів механічного, електронного або іншого копіювання.

4.5. Функціонал мобільного застосунку може розширюватися поступово і деякі функції та можливості, описані в цих Умовах, можуть бути недоступними на момент їх оприлюднення.

5. ПРАВА ТА ОБОВ'ЯЗКИ СТОРІН

5.1. Клієнт зобов'язаний:

5.1.1. Забезпечити недоступність пароля для третіх осіб, в тому числі членів власної сім'ї, родини, зокрема не зберігати у відкритому вигляді пароль для входу до мобільного застосунку на будь-якому носії (паперовому, електронному тощо).

5.1.2. Зберігати авторизаційні дані у місцях, недосяжних для сторонніх осіб та:

- у випадку підозри на несанкціонований доступ до авторизаційних даних, терміново припинити використання мобільним застосунком, довести це до відома Банку, шляхом звернення до відділення Банку або до контакт-центру, з метою здійснення заходів для запобігання шахрайських дій тощо;
- у випадку втрати (крадіжки) авторизаційних даних та/або фінансового номеру мобільного телефону Клієнта, на який здійснюється відправлення одноразового коду, або при виявленні випадків проведення за рахунком Клієнта операцій, що ним не санкціоновані, негайно звернутися до контакт-центру Банку з вимогою заблокування доступу до мобільного застосунку. У разі звернення в Банк за телефоном контакт-центру, Клієнт зобов'язаний пройти процедуру ідентифікації та за необхідності надати Банку додаткові відомості про себе. Фінансовий номер мобільного телефону Клієнта може бути змінений Клієнтом лише після особистого звернення Клієнта на відділення з письмовою заявою, складеною за формою Банку та проведення повторної ідентифікації Клієнта.
- не розголошувати нікому, в тому числі членам власної родини, авторизаційні дані для доступу до мобільного застосунку;
- не зберігати записані авторизаційні дані доступу до мобільного застосунку на будь-якому паперовому чи цифровому носієві;
- забезпечити захист свого мобільного телефону та SIM-картки, на номер якого надсилаються одноразові коди підтвердження операцій;
- забезпечити антивірусну безпеку своїх інформаційних систем (безперервне використання та своєчасне оновлення антивірусних програм на смартфонах, планшетах тощо), за допомогою яких Клієнт виконує вхід до мобільного застосунку;
- негайно змінити пароль в мобільному застосунку у випадку якщо пароль, або його частина стала відома іншій особі;
- налаштовувати електронні повідомлення про рух коштів на банківському(-их) рахунку(-ах) та ЕПЗ для контролю несанкціонованого використання коштів;
- дотримуватися загальних правил безпеки: не поширювати реквізити своїх ЕПЗ, дані щодо тимчасових одноразових кодів та дані щодо пароля, не проводити операції з рахунками в місцях загального доступу, не використовувати WI-FI у публічних місцях. Номер мобільного (фінансового) телефону Клієнта може бути змінений Клієнтом лише після особистого звернення Клієнта на відділення з письмовою заявою, складеною за формою Банку та проведення повторної ідентифікації Клієнта.

5.1.3. У разі зміни зареєстрованого в Банку мобільного номера телефону, зазначеного в Заві-

договорі про приєднання/Анкеті фізичної особи, в тому числі, фізичної особи, яка здійснює незалежну професійну діяльність, необхідно особисто звернутись до Банку та надати відповідну Заяву-договір про внесення змін до Заяви-договору про приєднання. Неповідомлення Клієнтом Банку про зміну номера мобільного телефону, звільняє Банк від будь-якої відповідальності, що може виникнути у зв'язку з відправленням Банком одноразового коду на попередній номер мобільного телефону Клієнта.

5.1.4. Здійснювати оплату банківських послуг, наданих за допомогою мобільного застосунку відповідно до чинних, на момент надання Банком відповідної банківської послуги, тарифів Банку. Укладанням Договору Клієнт безвідклично доручає, а Банк має право здійснювати списання грошових коштів з рахунку Клієнта в рахунок оплати наданих банківських послуг за допомогою мобільного застосунку, за виключенням рахунків строкових вкладів (депозитів). Списання коштів з рахунку Клієнта здійснюється виключно в разі наявності на такому рахунку суми, достатньої для оплати наданої Банком послуги.

5.1.5. На вимогу Банку надати належним чином оформлені документи на підтвердження операції/дії/документа в паперовій формі, що попередньо були передані Клієнтом до Банку за допомогою мобільного застосунку, а також надати додаткову інформацію та відповідні документи щодо операцій Клієнта.

5.1.6. Для належного отримання послуг за Договором своєчасно встановлювати доступні оновлення операційної системи і додатків на своєму мобільному пристрої, що використовується для підключення телефону Клієнта до мобільного застосунку.

5.1.7. Нести відповідальність за усі дії та операції, здійснені у мобільному застосунку, встановленому на будь-якому мобільному пристрої Клієнтом та/або за його згодою чи за його сприяння. Під згодою Клієнта та/або сприянням Клієнта мається на увазі успішний вхід в мобільний застосунок з використанням автентифікаційних даних Клієнта.

5.1.8. Інші обов'язки, передбаченні Договором та чинним законодавством України.

5.2. Клієнт має право:

5.2.1. Користуватись повним комплексом послуг, які надаються через мобільний застосунок на умовах, передбачених Договором та цією Умовою.

5.2.2. Самостійно розпоряджатися коштами на своїх рахунках в порядку, встановленому законодавством України, нормативно-правовими актами Національного банку України та механізмами, реалізованими в мобільному застосунку на умовах Договору та цієї Умови.

5.2.3. Здійснювати активацію мобільного застосунку в будь-який час за власним бажанням 24 години на добу 7 днів на тиждень, за виключенням періодів проведення регламентних робіт Банком, про які Банк зобов'язаний повідомити Клієнтів відповідним оголошенням на сайті Банку, в стрічці новин мобільного застосунку та/або SMS-повідомленням.

5.2.4. В будь-який час за власним бажанням і на власний розсуд змінити пароль для входу в мобільний застосунок.

5.2.5. Формувати, підтверджувати операції/дії/документи у мобільному застосунку та вимагати від Банку їх виконання відповідно до умов Договору, із застосуванням положень цих Умов та відповідно до чинного законодавства України та нормативно-правових актів Національного банку України.

5.2.6. Інші права передбачені Договором та чинним законодавством України.

5.3. Обов'язки Банку:

5.3.1. Приймати до виконання та виконувати операції/дії/документи Клієнта, підписані електронним підписом, оформлені та надані Клієнтом відповідно до Договору, нормативно-правових актів Національного банку України та чинного законодавства України.

5.3.2. У випадку зміни умов та/або порядку надання банківських послуг за допомогою мобільного застосунку, визначених цими Умовами, повідомити про це Клієнта не пізніше, ніж за 10 (десять) календарних днів до набрання чинності нової редакції Умов шляхом розміщення відповідного повідомлення на сайті Банку, у відділеннях Банку або Viber розсилкою. Ініціюючи будь-яку операцію за допомогою мобільного застосунку після набрання чинності нової редакції цих Умов, Клієнт підтверджує, що він ознайомився, чітко усвідомив та цілком погодився з такою редакцією Умов та прийняв їх до виконання.

5.3.3. Зберігати таємницю щодо операцій Клієнта та надавати відомості по них третім особам

тільки у випадках, передбачених законодавством України та нормативно-правовими актами Національного банку України.

5.3.4. Інші обов'язки, передбаченні Договором та законодавством України.

5.4. Права Банку:

5.4.1. На виконання зобов'язань Клієнта за Договором здійснювати дебетовий переказ (договірне списання) коштів з рахунків Клієнта відповідно до умов Договору, із застосуванням положень цих Умов, та відповідно до нормативно-правових актів Національного банку України та чинного законодавства України.

5.4.2. Відмовити Клієнту у прийомі та/або виконанні операції/дії/документа у наступних випадках:

- у разі недостатності на рахунку Клієнта, з якого здійснюється переказ коштів, суми коштів, необхідної для здійснення переказу та/або суми, необхідної для сплати комісійної винагороди за здійснення такої операції (якщо це передбачено тарифами Банку, чинними на момент виконання операції);
- у разі невідповідності операції/дії/документа чинному законодавству України, нормативно-правовим актам Національного банку України, умовам Договору, цим Умовам;
- у разі, недотримання Клієнтом вимог законодавства у сфері запобігання та протидії ВК/ФТ;
- якщо сума переказу перевищує ліміт, що встановлений згідно нормативно-правоих актів Національного банку України, чинного законодавства України та платіжною системою;
- встановлення Клієнту неприйнятно високого ризику або ненадання Клієнтом документів чи відомостей необхідних для здійснення заходів належної перевірки Клієнта;
- у разі, якщо у Банку виникає сумнів стосовно того, що Клієнт виступає від власного імені та власноруч підтверджує або вводить одноразовий код для виконання операції/дії/документа;
- у разі наявності арештів рахунку Клієнта та інших боргових зобов'язань.

5.4.3. Здійснювати модернізацію мобільного застосунку та/або впроваджувати його більш досконалі версії.

5.4.4. Здійснювати тимчасову зупинку роботи мобільного застосунку для проведення профілактичних робіт, про які Банк зобов'язаний заздалегідь повідомити Клієнта відповідним оголошенням на сайті Банку/в мобільному застосунку та/або SMS-повідомленнями або Viber розсилкою.

5.4.5. В рамках дистанційного обслуговування Банк надає Клієнту інформацію про банківське обслуговування фінансового характеру, шляхом направлення SMS- повідомлень, в тому числі шляхом направлення Push-повідомлень в мобільний додаток.

5.4.6. Вимагати у передбачених законодавством України випадках надання Клієнтом додаткової інформації та відповідних документів щодо операцій Клієнта.

5.4.7. За власною ініціативою та на власний розсуд змінити ці Умови за умови повідомлення Клієнта шляхом розміщення такої редакції на офіційному сайті Банку, у відділеннях Банку у строк, передбачений Договором. Ініціюванням будь-якої операції за допомогою мобільного застосунку після набрання чинності нової редакції Договору/цих Умов Клієнт підтверджує своє ознайомлення та погодження з такою редакцією Умов та прийняття їх до виконання.

5.4.8. Вимагати від Клієнта оплати послуг згідно з тарифами Банку та умов Договору.

5.4.9. З метою запобігання шахрайських та ризикових операцій Клієнта, Банк має право протягом терміну дії Договору встановлювати геопозиціонування телефону Клієнта, фінансовий номер якого вказаний у Договорі, а також використовувати інформацію про місцезнаходження Клієнта, отриманої Банком на підставі геопозиціонування телефону. У випадку неможливості підтвердження легітимності операції, Банк має право обмежити проведення операцій Клієнта.

5.4.10. Без пояснення причин відхилити реєстрацію Клієнта/запропонувати звернутися до відділення Банку.

5.4.11. Інші права, передбаченні Договором та чинним законодавством України.

6. ВІДПОВІДАЛЬНІСТЬ СТОРІН ТА ВИРІШЕННЯ СПОРІВ

6.1. За невиконання або неналежне виконання своїх зобов'язань, передбачених Договором, цими Умовами, Банк та Клієнт несуть відповідальність згідно з чинним законодавством України.

6.2. Клієнт несе усі ризики та відповідальність:

- пов'язану з розголошенням пароля для входу в мобільний застосунок, секретної інформації, яка використовується для відновлення пароля для входу до мобільного застосунку, а також будь-якої інформації про свої рахунки, що є банківською таємницею, у разі здійснення доступу до мобільного застосунку не з власного мобільного пристрою;
- пов'язану зі здійснення доступу до мобільного застосунку через мобільний пристрій, що необладнаний засобами антивірусного та мережевого захисту, а також через не оновлене до останньої версії програмного забезпечення мобільного застосунку;
- пов'язану з використанням для доступу до мобільного застосунку незахищених та публічних мереж Wi-Fi;
- за проведені операції в мобільному застосунку, який встановлено на мобільний пристрій з наявністю шкідливого програмного забезпечення;
- за надійність введеного пароля для доступу до мобільного застосунку, його збереження та недоступність третім особам. При цьому, Банк не несе жодної відповідальності за використання даних Клієнта, які використовуються для доступу до мобільного застосунку будь-якими третіми особами;
- за всі операції, що проводяться Клієнтом та/або третіми особами з відома або без відома Клієнта під час використання мобільного застосунку для здійснення фінансових операцій, в тому числі в разі якщо програмне забезпечення та/або мобільний пристрій Клієнта, з використанням яких здійснюється доступ до даних послуг, були схильні до модифікації, що порушує угоду Клієнта, укладену між Клієнтом і виробником програмного забезпечення та/або мобільного пристрою, а також у разі якщо на мобільному пристрої, що використовується для підключення телефону Клієнта до мобільного застосунку був активований режим для розробників, та якщо мобільний пристрій був замінений на інший;
- за розголошення адреси електронної пошти/зареєстрованого номера мобільного телефону для доступу до мобільного застосунку, збереження пароля, а також за всі дії, вчинені з використанням мобільного застосунку;
- не повідомлення Банку про будь-який випадок несанкціонованого доступу до мобільного застосунку та/або про будь-яке порушення безпеки третіми особами.

Клієнт усвідомлює та приймає на себе усі ризики, пов'язані з використанням третіми особами мобільного пристрою Клієнта або фінансового номера телефону через його крадіжку або створення дублікату SIM-карти фінансового номера телефону.

Клієнт усвідомлює та приймає на себе усі ризики щодо можливості авторизації сторонньою особою у мобільному застосунку за допомогою біометричних даних. Будь яку особу, що використала біометричні дані як засіб автентифікації/верифікації держателя ЕПЗ під час використання мобільного застосунку Банк безумовно вважає Клієнтом і не несе відповідальності за дії такої особи, навіть якщо такі дані будуть оскаржуватися.

6.3. Банк не несе відповідальності:

- у разі здійснення Клієнтом дій для доступу до мобільного застосунку/інших дій в мобільному застосунку, що не відповідають вимогам Банку;
- за помилки, затримки, неможливість здійснення Клієнтом доступу до мобільного застосунку, а також всі негативні наслідки (збитки, спричинені Клієнту та/або третім особам), що пов'язані з:
  - незадовільною якістю послуг надання Клієнту доступу до мережі Інтернет та інших каналів зв'язку, необхідних для користування мобільним застосунком;
  - неналежним функціонуванням програмного забезпечення, що застосовується для роботи з мобільним застосунком;
  - неналежним антивірусним та/або мережевим захистом мобільного пристрою, що

використовується Клієнтом;
- несправністю та/або дефектами обладнання Клієнта, його неправильного або несанкціонованого використання;
- ненадходженням SMS-повідомлення/Viber розсилки Клієнту через мережу оператора мобільного зв'язку з незалежних від Банку причин;
- припиненням надання послуг за Договором внаслідок настання та дії обставин непереборної сили (форс-мажор), що унеможливлюють подальше надання послуг за Договором та виникнення інших незалежних від Банку обставин;

- за ушкодження обладнання Клієнта або інформації, що зберігається в обладнанні Клієнта, за безпеку програмного забезпечення Клієнта (мобільного телефону тощо) від різного роду вірусів й інших пошкоджень;
- за відмову у проведенні операції/дії/документа, що підписані одноразовим кодом, та надані через мобільний застосунок, якщо вони знаходяться не в межах залишку грошових коштів на відповідному рахунку Клієнта та не відповідають вимогам законодавства України;
- за невиконання операції/дії/документа Клієнта, якщо на рахунок було накладено арешт або операції по ньому були призупинені Банком в порядку, передбаченому до умов Договору, цих Умов та відповідно до чинного законодавства України;
- за виконання операції/дії/документа Клієнта, зокрема на списання коштів з рахунку Клієнта, що були незаконно (несанкціоновано) оформлені та надані до Банку за допомогою мобільного застосунку, якщо Клієнтом накладено ЦВП та/або одноразовий код є вірним;
- за наслідки несвоєчасного повідомлення Клієнтом Банку про втрату (крадіжку) автентифікаційних даних та/або втрати контролю над фінансовим номером, на який здійснюється відправлення повідомлення про невірно проведені операції та про спроби несанкціонованого доступу до рахунку Клієнта (або про здійснення такого доступу), зокрема за наслідки всіх операцій, здійснених за допомогою мобільного застосунку з використанням автентифікаційних даних та/або фінансового номера до моменту повідомлення про це Банк;
- у випадку зміни законодавства України чи прийняття нових законів, інших нормативно правових актів, які змінюють чи припиняють правовідносини, що регулюються Договором та/або цими Умовами;
- у випадку виникнення між Клієнтом та Банком спорів та розбіжностей, що випливають із Договору та/або Умови, Сторони докладуть усіх зусиль для вирішення їх шляхом переговорів. У випадку неможливості вирішити спір шляхом переговорів, такий спір має бути вирішений у порядку, передбаченому законодавством України.