ЗАТВЕРДЖЕНО

Рішенням Правління
ПУБЛІЧНОГО АКЦІОНЕРНОГО
ТОВАРИСТВА
АКЦІОНЕРНИЙ БАНК «ПІВДЕННИЙ»

Рішення №32 від «27» березня 2026 року
набирає чинності з «27» березня 2026 року

ПРАВИЛА
КОРИСТУВАННЯ СИСТЕМАМИ ДИСТАНЦІЙНОГО ОБСЛУГОВУВАННЯ ФІЗИЧНИХ ОСІБ ПУБЛІЧНОГО АКЦІОНЕРНОГО ТОВАРИСТВА АКЦІОНЕРНОГО БАНКУ «ПІВДЕННИЙ»

м. Одеса, 2026 рік

1. ВИЗНАЧЕННЯ, ТЕРМІНИ, СКОРОЧЕННЯ

«CVV2/CVC2-код» – 3 цифри на зворотній стороні платіжної картки. Оригінальний набір символів, відомий лише Клієнту, потрібний для його ідентифікації при здійсненні операцій за допомогою Інтернет-сервісів. Клієнт зобов'язаний забезпечити/гарантувати неможливість отримання третіми особами інформації про CVV2/CVC2-код. Ризик і всю відповідальність за несанкціоноване використання CVV2/CVC2-коду несе виключно Клієнт;
BankID (Система BankID) - комплекс програмно-технічних засобів та організаційно-технологічних заходів для забезпечення дистанційної ідентифікації користувачів під час інформаційної взаємодії між абонентами (Портал Послуг та Автоматизована Банківська Система) в електронній формі з використанням банківських систем дистанційного обслуговування;
IBAN (International Bank Account Number) – міжнародний номер банківського рахунку;
MOBI-CARD – система інформаційних повідомлень, яка надає можливість Клієнту/Держателю ПК Банку цілодобово отримувати інформацію про рух коштів по КР, у вигляді SMS-повідомлень за допомогою Фінансового номера телефону, підключеного до будь-якого українського оператора мобільного зв'язку;
MASTERPASS ВІД MASTERCARD® - електронний платіжний сервіс, що зберігає усі дані платіжних карток в одному місці, шляхом створення власного електронного гаманця, для розрахунків онлайн. До електронного гаманця Masterpass можна додати ПК як МПС Mastercard, так і МПС VISA. Створення власного електронного гаманця полягає у створенні облікового запису та реєстрації платіжної картки. Жоден онлайн-ресурс (мобільний застосунок, інтернет-сайт та ін.) не зберігає дані платіжної картки на своїх ресурсах. Ідентифікатором електронного гаманця, до якого прив'язана платіжна картка, виступає логін Клієнта (електронна адреса або номер мобільного телефону). Безпеку збереження даних платіжної картки, що вводилися Клієнтом при створенні електронного гаманця та пов'язаного з нею ідентифікатора електронного гаманця гарантує Mastercard. Детальна інформація про сервіс за посиланнями: https://masterpass.com/uk-ua.html та https://www.masterpass.com.ua/TermsAndConditions.aspx;
NFC – Near Field Communication – технологія бездротового високочастотного зв'язку малого радіусу дії (за один дотик). Ця технологія дає можливість обміну даними між пристроями (смартфонами та безконтактними платіжними терміналами);
SE – Secure Element – це сертифікована мікросхема для безпечного зберігання платіжної інформації на пристрої Apple (iPhone, iPad, Apple Watch, Apple Mac), Garmin (згідно модельного ряду підтримуваних пристроїв Garmin), Android (згідно модельного ряду підтримуваних пристроїв Android). Дані платіжного токена, що створюється при додаванні платіжної картки до сервісу Apple Pay та Garmin Pay зберігаються в Secure Element. Дані в модулі Secure Element повністю ізольовані від операційної системи iOS, watchOS та macOS, Garmin OS, а також ніколи не зберігаються на серверах Apple, у тому числі в резервній копії iCloud, та Garmin.
SMS-ПОВІДОМЛЕННЯ – послуга електронних повідомлень - технологія, що дозволяє відправляти та отримувати повідомлення за допомогою зокрема відповідного програмного застосунку, який включає в т.ч. VoIP технологію, послуг українського оператора мобільного зв'язку за наявності відповідного засобу мобільного зв'язку (зокрема, мобільного (сотового) телефону, планшетного пристрою, ПК), а також, інших засобів миттєвої передачі повідомлень (зокрема Viber, PUSH-сповіщення), інформаційного обміну;
PIN-код доступу — набір 4-х цифр, відомий лише Користувачеві Застосунку «PIVDENNY ONLINE», необхідний для автентифікації Клієнта при вході до Застосунку;
PUSH-сповіщення — це короткі повідомлення, які Застосунок «PIVDENNYI ONLINE» надсилає на мобільні пристрої своїм зареєстрованим Клієнтам, які дали дозвіл на отримання таких повідомлень. З їх допомогою Клієнт може отримувати інформацію щодо руху коштів, сервісних операцій, повідомлень Банку та переходити до відповідного розділу/функціоналу в Застосунку.
АВТЕНТИФІКАЦІЯ – процедура встановлення за допомогою Системи та Мобільного застосунку «PIVDENNY ONLINE» достовірності ідентифікатора користувача Системи, Мобільного застосунку «PIVDENNY ONLINE». Для цілей використання мобільного застосунку сервісів: «Google Pay», «Apple Pay» та «Garmin Pay» - процедура підтвердження повноважень (надання прав доступу) Держателя Платіжної картки до сервісів: «Google Pay», «Apple Pay» та «Garmin Pay»;
АВТОРИЗАЦІЯ ПО ВІДБИТКАМ ПАЛЬЦІВ – вхід у мобільний застосунок «PIVDENNY ONLINE» за допомогою технології FingerPrint (за наявності дактилоскопічного сканеру у мобільному пристрої);
АВТОРИЗАЦІЯ ЧЕРЕЗ СИСТЕМУ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ ЛЮДИНИ – вхід у мобільний застосунок «PIVDENNY ONLINE» за допомогою технології Face ID (за наявності функції у мобільному пристрої);
АКТИВНИЙ ПРИСТРІЙ – мобільний пристрій з якого Клієнтом було виконано останню успішну автентифікацію у Застосунку «**PIVDENNY ONLINE»**, та не виконано вихід із Застосунку відповідно до функціоналу;
АКТИВНИЙ РЕЖИМ РОБОТИ В СИСТЕМІ ДИСТАНЦІЙНОГО ОБСЛУГОВУВАННЯ «ПІВДЕННИЙ MYBANK» – набір функціональних можливостей, доступних Клієнту в Системі дистанційного обслуговування «**ПІВДЕННИЙ MYBANK**», який дозволяє перегляд власних рахунків та деталей рахунків, а також формування виписок та передбачає можливість здійснювати розрахунки у безготівковій формі та/або переказ коштів на інші рахунки, а також інші операції, передбачені чинним законодавством та ДКБОФО;
БАНК – ПУБЛІЧНЕ АКЦІОНЕРНЕ ТОВАРИСТВО АКЦІОНЕРНИЙ БАНК «ПІВДЕННИЙ» (скорочене найменування - Акціонерний банк «Південний») і всі його Відокремлені підрозділи (відділення);
БІОМЕТРИЧНА АВТЕНТИФІКАЦІЯ – спосіб верифікації Клієнта за протоколом 3-D Secure під час здійснення транзакції в мережі Інтернет в Системі дистанційного обслуговування «ПІВДЕННИЙ MYBANK» та Мобільному застосунку «PIVDENNY ONLINE» шляхом авторизації за допомогою технології FingerPrint/Face ID або введення паролю для входу. Дана технологія доступна лише за транзакціями Mastercard Identity Check та Visa Secure;
ДИСТАНЦІЙНИЙ ОБМІН ВАЛЮТ (ОБМІН ВАЛЮТ У СИСТЕМІ) – послуга з купівлі, продажу та обміну (конвертації) валют, що надається Клієнту у Системі дистанційного обслуговування «ПІВДЕННИЙ MYBANK» та Мобільному застосунку «PIVDENNY ONLINE», що містить можливість для Клієнта оформити Дистанційне розпорядження на обмін валют протягом

дня із наступним списанням/зарахуванням коштів Банком з/на відповідні поточні рахунки (в тому числі КР) Клієнта за умови прийняття його Банком для виконання в той же день;

ДИСТАНЦІЙНЕ РОЗПОРЯДЖЕННЯ НА ОБМІН ВАЛЮТ (ЗАЯВКА НА КУПІВЛЮ/ПРОДАЖ/ОБМІН (КОНВЕРТАЦІЮ) ВАЛЮТИ У СИСТЕМІ) – електронне розпорядження, що складається та надається Клієнтом у Системі дистанційного обслуговування «ПІВДЕННИЙ MYBANK» та у Мобільному застосунку «PIVDENNY ONLINE». Містить суми операції, що будуть списані/зараховані на рахунки Клієнта, номери рахунків Клієнта для здійснення операції та курс Дистанційного обміну валют;

ДИСТАНЦІЙНЕ РОЗПОРЯДЖЕННЯ РАХУНКОМ – операції з розпорядження Рахунком та/або коштами, які знаходяться на Рахунку, шляхом передачі Клієнтом Електронних документів, підтверджених Разовим паролем, за допомогою Системи та/або Мобільного застосунку «PIVDENNY ONLINE» через мережу Інтернет без безпосереднього звернення до Банку;

ДОГОВІР КОМПЛЕКСНОГО БАНКІВСЬКОГО ОБСЛУГОВУВАННЯ ФІЗИЧНИХ ОСІБ (ДКБОФО) – договір між Банком і Клієнтом (включаючи Правила користування та обслуговування платіжних карток, всі додатки до нього, Тарифи, Депозитна програма, Ліміти за операціями з використанням платіжного інструменту, заяви тощо), який укладається зокрема шляхом подання Клієнтом відповідної заяви (у тому числі в електронному вигляді) на отримання банківської послуги та/або підписання/подання Клієнтом відповідної Заяви-Договору про надання банківського продукту/послуги (включаючи Договір банківського рахунку, Договір банківського вкладу, тощо) та приєднання до Договору комплексного банківського обслуговування, що є акцептуванням Публічної пропозиції Банку (оферти), в тексті також – Договір. Примірник Договору комплексного банківського обслуговування, включаючи його мобільну версію, розміщується в електронному вигляді - на Офіційному сайті Банку для ознайомлення Клієнтів і надається Клієнту в момент підписання Заяви-Договору про надання банківського продукту/послуги у спосіб, обраний ним із запропонованих надавачем фінансових послуг, який дає змогу встановити дату надання цього Договору, з використанням контактних даних, зазначених Клієнтом. Усі редакції ДКБОФО зберігаються на сайті Банку із зазначенням строку їх дії у порядку та протягом строку, встановлених нормативно-правовими актами НБУ, але не менше трьох років з дати припинення дії останнього з ДКБОФО у відповідній редакції. Прийняття Клієнтом положень Договору комплексного банківського обслуговування здійснюється Клієнтом також шляхом вчинення Клієнтом відповідних дій, що підтверджують його намір користуватись певними банківськими послугами чи продуктами, зокрема за допомогою Системи дистанційного обслуговування «ПІВДЕННИЙ MYBANK» та Мобільного застосунку «PIVDENNY ONLINE» (укладення Договору шляхом вчинення певних дій);

ЕЛЕКТРОННИЙ ДОГОВІР – Заява-Договір або інший правочин щодо надання банківських послуг, який укладається між Банком та Клієнтом в Системі дистанційного обслуговування «ПІВДЕННИЙ MYBANK» та\або Мобільному застосунку «PIVDENNY ONLINE» у формі Електронного документу, підписання якого з боку Клієнта підтверджується Електронним підписом Клієнта (Разовим паролем);

ЕЛЕКТРОННИЙ ДОКУМЕНТ – створений в системі дистанційного обслуговування «ПІВДЕННИЙ MYBANK» та\або Мобільному застосунку «PIVDENNY ONLINE» документ, інформація в якому зафіксована у тому числі у вигляді електронних даних, включаючи електронний підпис Клієнта (Разовий пароль). До Електронних документів зокрема відносяться Електронні договори, Електронні платіжні інструкції, Доручення на договірне списання, повідомлення та інші документи, можливість створення яких передбачена в Системі дистанційного обслуговування «ПІВДЕННИЙ MYBANK» та\або Мобільному застосунку «PIVDENNY ONLINE»;

ЕЛЕКТРОННА ПЛАТІЖНА ІНСТРУКЦІЯ – документ, інформацію в якому представлено у формі електронних даних, та який містить розпорядження Клієнта переказати грошові кошти в межах Банку або в інші банки України або банки за кордоном, з одного його рахунку на інший його рахунок або на рахунок третьої особи, а також містить відповідні реквізити, в т.ч передбачені нормативно-правовими актами НБУ, який може бути сформований, переданий, збережений і перетворений у візуальну форму за допомогою Системи та/або Мобільного застосунку «PIVDENNY ONLINE, та що підтверджений (підписаний) Електронним підписом, яким відповідно до ДКБОФО, є Разовий пароль;

ЕЛЕКТРОННИЙ ПІДПИС – дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача (Клієнта) цих даних. Сторони домовились, що згенерований Банком Разовий пароль та направлений Клієнту під час здійснення платіжних операцій в Системі дистанційного обслуговування «ПІВДЕННИЙ MYBANK» та\або Мобільному застосунку «PIVDENNY ONLINE», банкоматі, а також здійснення в програмних комплексах будь-яких маніпуляцій, спрямованих на успішне завершення платежу та/або отримання будь-яких послуг, прирівнюється до електронного підпису Клієнта. Підписання електронним підписом документів з боку Клієнта в Системі дистанційного обслуговування «ПІВДЕННИЙ MYBANK» та\або Мобільному застосунку «PIVDENNY ONLINE» здійснюється зокрема шляхом авторизації клієнта за допомогою Фінансового номеру телефону та Разового пароля. Банк генерує Разовий пароль і надсилає його клієнтові в тілі повідомлення на Фінансовий номер телефону із зазначенням інформації, яка буде ним підтверджуватися. Для підтвердження згоди Клієнт передає у відповіді отриманий Разовий пароль або вводить цей пароль у відповідному рядку використовуваного сервісу. Сторони визнають Разовий пароль, а також відповідну позначку, що проставляється Клієнтом в Системі дистанційного обслуговування «ПІВДЕННИЙ MYBANK» та\або Мобільному застосунку «PIVDENNY ONLINE» для підтвердження відповідної інформації та/або надання згоди з боку Клієнта - електронним підписом Клієнта, що є аналогом власноручного підпису. Підписувач, який створює електронний документ з електронним підписом, цим самим засвідчує, що ознайомився з усім текстом документа, повністю зрозумів його зміст, не має заперечень до тексту документа (або його заперечення внесені як окремий реквізит документа) і свідомо застосовував свій електронний підпис у контексті, передбаченому документом (підписав, затвердив, погодив, завізував, засвідчив, ознайомився);

КЛІЄНТ – фізична особа (резидент або нерезидент України), яка уклала із Банком ДКБОФО та/або одержує послуги від Банку на умовах, визначених ДКБОФО та/або звертається за отриманням послуг до Банку;

КОД АВТОРИЗАЦІЇ – набір цифр або букв і цифр, який формується і надається емітентом або юридичною особою – учасником платіжної системи, яка діє за його дорученням, за результатами авторизації;

ЛОГІН – унікальний набір символів, що ідентифікує Клієнта у Системі дистанційного обслуговування «ПІВДЕННИЙ MYBANK» та\або фінансовий чи основний номер телефону у Мобільному застосунку «PIVDENNY ONLINE та є інформацією обмеженого доступу і може бути повідомлений Клієнтом виключно уповноваженому працівнику Банку. Клієнт зобов'язаний забезпечити/гарантувати неможливість отримання третіми особами інформації про Логін. Ризик і всю відповідальність за несанкціоноване використання Логіна несе виключно Клієнт;

МИТТЄВИЙ ПЛАТІЖ (МИТТЄВИЙ КРЕДИТОВИЙ ПЕРЕКАЗ) – ініційований Клієнтом в Мобільному застосунку **«PIVDENNY ONLINE»** переказ коштів за реквізитами рахунку отримувача в форматі IBAN, який виконується Банком невідкладно (протягом 10 секунд) з моменту прийняття платіжної інструкції в будь-яку з 24 годин будь-якого календарного дня, починаючи з 07.08.2025 року;

МОБІЛЬНИЙ ЗАСТОСУНОК «PIVDENNY ONLINE» - сервіс Банку для Мобільного пристрою, що працює під операційною системою iOS/Android за допомогою якого Клієнту надаються банківські послуги та інформація стосовно обслуговування Клієнта в Банку, здійснюється Дистанційне розпорядження Рахунками та виконуються платежі та інші операції Клієнтом. Всі операції за допомогою Мобільного застосунку **«PIVDENNY ONLINE»** здійснюються згідно з ПРАВИЛАМИ КОРИСТУВАННЯ МОБІЛЬНИМ ЗАСТОСУНКОМ **«PIVDENNY ONLINE»**;

МОБІЛЬНИЙ ПРИСТРІЙ – мобільний телефон (планшетний комп'ютер, смарт-годинник тощо) з розширеною функціональністю, що працює під операційною системою iOS чи Android, на які дозволяється встановлення додаткових програм\застосунків;

ПАРОЛЬ ДЛЯ ВХОДУ – унікальна послідовність із символів і цифр, використовувана для ідентифікації Клієнта в Системі дистанційного обслуговування **«ПІВДЕННИЙ MYBANK»** та\або Мобільному застосунку «PIVDENNY ONLINE», та яка використовується Клієнтом при вході в Систему дистанційного обслуговування **«ПІВДЕННИЙ MYBANK»** та\або у Мобільний застосунок «PIVDENNY ONLINE» на постійній основі. Клієнт встановлює цей пароль самостійно при першому вході в Систему дистанційного обслуговування **«ПІВДЕННИЙ MYBANK»** та може змінити його в будь-який момент. При авторизації за допомогою Технології FingerPrint/Face ID, PIN-коду доступу до Мобільного застосунку «PIVDENNY ONLINE» розшифровує збережені Логін та Пароль для входу (які зберігає у зашифрованому вигляді) і Користувач входить з ними в систему;

ПЛАТІЖНА ІНФОРМАЦІЯ CLICK TO PAY – це сукупність ідентифікаційної та платіжної інформації про Клієнта, яку він самостійно передає при створенні профіля клієнта Click to Pay, або яку передає Банк до МПС Visa/ MasterCard від імені Клієнта. До переліку даних, необхідних для створення профілю клієнта Click to Pay входить: прізвище, ім'я та по батькові; номер ПК та термін дії; інформація для виставлення рахунків та доставки замовлення; дійсна адреса електронної пошти Клієнта (ця інформація може передаватися Клієнтом до МПС Visa/ MasterCard тільки у випадку самостійного створення профілю клієнта в Click to Pay); номер телефону Клієнта (у випадку, якщо створення профіля клієнта Click to Pay виконує Банк, він передає Фінансовий номер телефону або основний номер телефону, який є унікальним ідентифікатором Клієнта в Click to Pay. Тобто Банк не може створити профіль Click to Pay для кількох Клієнтів з однаковим номером телефону); та іншу інформацію, пов'язану зі здійсненням платежів в сфері електронної комерції за допомогою ПК МПС Visa/ MasterCard;

ПРОГРАМА ВИНАГОРОД MASTERCARD (ПРОГРАМА ВИНАГОРОД) – це Програма винагород, організована ПС MasterCard для фізичних осіб - клієнтів Банку, основана на Нарахуванні балів Держателю ПК MasterCard. При оплаті товарів, робіт, послуг на території України та за її межами з використанням ПК MasterCard, Клієнту нараховуються бали, які в подальшому можливо обміняти на винагороди від Програми винагород «MasterCard Rewards»;

РАЗОВИЙ ПАРОЛЬ (ДИНАМІЧНИЙ, ОТР-ПАРОЛЬ) – пароль, що є електронним підписом Клієнта, аналогом власноручного підпису Клієнта на Електронному документі, який генерується та надсилається Клієнту у повідомленні на Фінансовий номер телефону Клієнта/ PUSH-сповіщенні у Системі та/або Мобільному застосунку «PIVDENNY ONLINE». Разовий пароль призначений зокрема для підтвердження операції з отримання ПК/ ПІН-коду, підписання відповідного документу та/або підтвердження відповідної операції при здійсненні Клієнтом Дистанційного розпорядження Рахунком, дійсний для підтвердження тільки того Електронного документа, по якому відповідний Разовий пароль був сформований, та не може бути використаний повторно для підтвердження (підписання) іншого Електронного документу;
Термін дії разового паролю після генерації складає 5 хвилин;

СЕРВІС «APPLE PAY» – система електронних платежів з Мобільних пристроїв, розроблена компанією Apple, за технологією SE, що дозволяє Клієнту виконувати операції оплати товарів (послуг) шляхом піднесення мобільного пристрою до Платіжного терміналу або в мережі Інтернет шляхом здійснення покупок в мобільних застосунках або в браузерних версіях Інтернет-магазинів. Вимоги до мобільного пристрою: операційна система iOS, watchOS або macOS. Технологію підтримує iPhone з 6-ї версії, та усі iPhone серії SE. Окрім суто Мобільних пристроїв (iPhone, iPad), технологія Apple Pay також доступна для використання на Apple Watch та Apple MacBook. Повний перелік пристроїв, що підтримує технологію Apple Pay, надає компанія Apple. Для користування технологію «Apple Pay» необхідно створити пароль та, за бажанням, налаштувати Face ID або Touch ID;

СЕРВІС «CLICK TO PAY» – це спосіб (механізм) оплати в режимі онлайн з удосконаленою платіжною технологією, який побудований на основі галузевого стандарту електронної комерції – EMV Secure Remote Commerce, та розумних систем безпеки від МПС Visa/ MasterCard. Сервіс для кожної із МПС розпочинає діяти з моменту його технічної реалізації та готовності Банку, про що Клієнти додатково інформуються на Сайті Банку;

СЕРВІС «GOOGLE PAY» – система електронних платежів з Мобільних пристроїв, розроблена компанією Google, за технологією HCE, що дозволяє Клієнту виконувати операції оплати товарів (послуг) шляхом піднесення Мобільного пристрою до платіжного терміналу або в мережі Інтернет шляхом здійснення покупок в мобільних застосунках або в браузерних версіях Інтернет-магазинів. Вимоги до Мобільного пристрою: операційна система Android (version 4.4+), функція NFC;

СЕРВІС «GARMIN PAY» – система електронних платежів з пристроїв, розроблена компанією Garmin за технологією SE, що дозволяє Клієнту виконувати операції оплати товарів (послуг) шляхом піднесення смарт-годинника Garmin до платіжного терміналу. Вимоги до пристрою: конкретні моделі смарт-годинника Garmin, що підтримують технологію. Мобільний пристрій

операційної системи Android або iOS для встановлення додатку Garmin Connect, для того, щоб додатки ПК до Garmin Pay. Мобільний пристрій не обов'язково має бути оснащеним функцією NFC;

СИСТЕМА ДИСТАНЦІЙНОГО ОБСЛУГОВУВАННЯ «ПІВДЕННИЙ MYBANK» – програмно-апаратний комплекс Банку, за допомогою якого Клієнту надаються банківські послуги та інформація стосовно обслуговування Клієнта в Банку, здійснюється Дистанційне розпорядження Рахунками та виконуються платежі та інші операції Клієнтом. Система дистанційного обслуговування **«ПІВДЕННИЙ MYBANK»** доступна для Клієнта через Сайт Банку за адресою: https://my.bank.com.ua;

ТЕХНОЛОГІЯ 3-D Secure – технологія, що використовується для підвищення безпеки платежів в мережі Інтернет та передбачає отримання Держателем електронного платіжного засобу Динамічного паролю, необхідного для здійснення платіжної операції. (сайти торговців, які підтримують цю технологію, мають позначення «***Verified by VISA***» або «***MasterCard SecureCode***»);

ТЕХНОЛОГІЯ EMV 3DS або 3-D Secure 2 – технологія, що використовується для підвищення безпеки платежів в мережі Інтернет та передбачає отримання Держателем електронного платіжного засобу Динамічного паролю, необхідного для здійснення платіжної операції, або підтвердження оплати шляхом Біометричної автентифікації. (Сайти торговців, які підтримують цю технологію, мають позначення «Mastercard ID Check» або «Visa Secure»;

ТЕХНОЛОГІЯ FINGERPRINT – процес ідентифікації за папілярним візерунком шкіри пальця (Відбиток пальця) з використанням дактилоскопічного сканеру у Мобільному пристрої;

ТЕХНОЛОГІЯ FACE ID – процес ідентифікації по об'ємно-просторовій формі обличчя людини, розроблений компанією Apple, який дозволяє розблокувати пристрій, здійснювати вхід у мобільні застосунки та інше;

ТЕХНОЛОГІЯ PASSKEY – технологія автентифікації, яка заміняє собою паролі та забезпечує більш безпечний вхід до застосунків та веб-сайтів. Для налаштування цього методу автентифікації Клієнт має виконати регламентовані дії безпосередньо в браузері на своєму девайсі. При цьому створюється пара криптографічних ключів. Вхід до особистого кабінету точки електронної комерції (Інтернет сайт або мобільний застосунок) відбувається шляхом підтвердження особи Клієнта на пристрої, наприклад, за допомогою сканування відбитка пальця, обличчя або введення PIN-коду самого пристрою;

ТИМЧАСОВИЙ ПАРОЛЬ ДЛЯ ВХОДУ – пароль, що генерується Системою та передається Клієнту за допомогою повідомлення на Фінансовий номер телефону Клієнта для автентифікації при першому вході Клієнта в Систему, а також після встановлення Клієнтом власного Паролю для входу – у разі втрати Клієнтом даних для автентифікації. Термін дії тимчасового паролю після генерації складає 30 днів;

ТОКЕН – цифрове представлення Платіжної картки, яке формується за фактом реєстрації Картки в Мобільному застосунку і зберігається в зашифрованому вигляді в захищеному сховищі Мобільного пристрою;

ТОКЕНІЗАЦІЯ – процес створення Токену і його прив'язування до ПК, що однозначно дозволяє визначити ПК, використану для здійснення операцій з використанням Сервісів Google Pay/Apple Pay/Garmin Pay та всіх можливих Інтернет-магазинів, що виступають запитувачами Токенів. Токенізація ПК здійснюється в процесі додавання ПК до мобільного застосунку, а її результатом виступає створений Токен в мобільному застосунку;

ФІНАНСОВИЙ НОМЕР ТЕЛЕФОНУ (ФІНАНСОВИЙ ТЕЛЕФОН, ФІНАНСОВИЙ НОМЕР) – це наданий Клієнтом/Держателем ПК номер мобільного телефону українського мобільного оператора, який підтверджується Клієнтом/Держателем ПК особисто з застосуванням ОТР-пароля або шляхом поглибленої верифікації в ЦЕНТРІ КЛІЄНТСЬКОЇ ПІДТРИМКИ, та встановлюється як єдиний номер телефону для проведення віддаленої верифікації Клієнта/Держателя ПК, оформлення банківських продуктів, підключення банківських послуг, отримання ПІН-коду до ПК, проведення та підтвердження фінансових операцій та інформування Банком Клієнта щодо них тощо. Після встановлення Банком Фінансового номеру, надані раніше Клієнтом/Держателем ПК інші номери телефонів надалі не використовуються для надання банківських послуг, проведення та підтвердження фінансових операцій та вважаються виключно контактними для можливості забезпечення комунікації Банку з Клієнтом/Держателем ПК. Надання фінансового номеру телефону Клієнта можливо представником Клієнта, виключно у разі надання документів, що підтверджують відповідні повноваження;

ЦЕНТР КЛІЄНТСЬКОЇ ПІДТРИМКИ – дистанційні канали обслуговування Банку, за допомогою яких Клієнт може цілодобово звернутися:

- за телефоном 0 800 30 70 30 (безкоштовно по Україні);
- за телефоном 0 482 30 70 30 (згідно тарифів оператора зв'язку);
- за допомогою інтернет-каналів голосового зв'язку з сайту Банку http://bank.com.ua/;
- через месенджери – Viber, Telegram, Messenger Facebook та live-чат на сайті Банку https://bank.com.ua;
- через Систему дистанційного обслуговування «ПІВДЕННИЙ MYBANK» та\або Мобільний застосунок «PIVDENNY ONLINE»;

ЧАТ/ЧАТ-БОТ – автоматизований сервіс дистанційного спілкування з клієнтами за допомогою месенджерів Viber, Telegram, Messenger Facebook та live-чат на сайті Банку https://bank.com.ua та отримання клієнтами довідкової інформації;

1. ПРАВИЛА КОРИСТУВАННЯ СИСТЕМОЮ ДИСТАНЦІЙНОГО ОБСЛУГОВУВАННЯ «ПІВДЕННИЙ MYBANK»

1.1. Підключення Клієнта до Системи здійснюється на підставі його заяви щодо надання доступу на обслуговування з використанням Системи дистанційного обслуговування «ПІВДЕННИЙ MYBANK» або шляхом здійснення Клієнтом самостійної реєстрації відповідно до умов ДОГОВОРУ КОМПЛЕКСНОГО БАНКІВСЬКОГО ОБСЛУГОВУВАННЯ ФІЗИЧНИХ ОСІБ (далі - ДКБОФО) та за умови наявності у Клієнта активної ПК.
Система дистанційного обслуговування «ПІВДЕННИЙ MYBANK» може використовуватися для підписання Електронних документів (у тому числі Електронних договорів), здійснення Договірного списання коштів з Рахунків Клієнта в Банку, а також надання інших послуг, передбачених ДКБОФО та Правилами користування Системою.
Перелік та доступність послуг, які Клієнт може отримати за допомогою Системи, їх зміст та порядок надання їх Клієнту, порядок роботи Системи можуть змінюватися в залежності від зміни функціональних можливостей Системи.
Підключення та надання доступу до Системи дистанційного обслуговування «ПІВДЕННИЙ MYBANK» здійснюється Банком виключно Клієнтів. Підключення та надання доступу до Системи дистанційного обслуговування «ПІВДЕННИЙ MYBANK» представникам Клієнта, а також малолітнім та неповнолітнім особам забороняється.
Підключення Клієнта до системи дистанційного обслуговування «ПІВДЕННИЙ MYBANK» можливо представником Клієнта, у разі надання документів, що підтверджують відповідні повноваження.
1.2. Самостійна реєстрація у Системі, здійснюється Клієнтом шляхом заповнення відповідної форми на сайті Системи. Для цього Клієнту необхідно ввести реквізити ПК (номер картки та CVV2/CVC2-код), після чого на ПК буде заблокована довільна сума від 1 до 3 грошових одиниць, в залежності від валюти рахунку (гривні, євро, долари США). Якщо за ПК Клієнта підключена послуга Mobi-card, він одразу отримає SMS-повідомлення з сумою блокування, яку необхідно ввести для продовження процедури реєстрації. Якщо послуга Mobi-card не підключена, Клієнту необхідно звернутися до ЦЕНТРУ КЛІЄНТСЬКОЇ ПІДТРИМКИ для уточнення суми блокування. Після завершення процедури реєстрації, сума блокування буде повернена на ПК Клієнта.
1.3. Крім того, на формі буде відображено прізвище, ім'я, по-батькові Клієнта, транслітеровані ім'я та прізвище, які будуть використовуватися в якості Логіна для входу в Систему, при цьому Клієнт має можливість змінити запропонований Логін. При цьому допустимі такі символи: літери латинського алфавіту, цифри, знаки «_» і «@». Довжина Логіна не може бути меншою ніж 6 символів. Додатково Клієнту необхідно ввести власну адресу електронної пошти, що буде використаний для відправлення повідомлень від Банку. Для завершення реєстрації потрібно натиснути «Підтвердити дані».
1.4. Після обробки заявки адміністратором Банку на Фінансовий номер телефону Клієнта, буде направлено повідомлення з Тимчасовим паролем для входу до Системи.
1.5. Надання Послуг в Системі здійснюється Банком у відповідності до Тарифів, чинних на момент проведення відповідної операції.
1.6. Перед початком обслуговування у Системі дистанційного обслуговування «ПІВДЕННИЙ MYBANK» Клієнт має ознайомитись із Посібником користувача Системи дистанційного обслуговування «ПІВДЕННИЙ MYBANK» для фізичних осіб Акціонерного банку «Південний» (надалі – Посібник), розміщеним на Сайті Банку https://bank.com.ua.
1.7. Режими роботи Системи
1.7.1. Клієнт отримує можливість обслуговуватись в Системі в обсязі, що визначений Банком, з урахуванням режимів Рахунків та законодавства України, з моменту у спішної автентифікації в Системі Клієнта. Для здійснення реєстрації та автентифікації в Системі Клієнт має здійснити відповідні дії, що визначені та регламентуються цими Правилами та Посібником.
1.7.2. Будь-яку особу, що використала Логін та/або Пароль доступу – для доступу до Системи (у томи числі за допомогою Технології FingerPrint/Face ID), та/або Разовий пароль – для здійснення операції у Системі, Банк безумовно вважає Клієнтом і не несе відповідальності за дії такої особи, якщо такі дії будуть оскаржуватись Клієнтом.
1.7.3. Банк зобов'язується виконувати доручення Клієнта про здійснення операцій за Рахунками, підтверджені Разовим паролем (за виключенням випадків обмеження розпорядження коштами відповідно до законодавства), за умови наявності коштів на Рахунках та коштів для сплати винагороди Банку за надання послуг, оплата яких передбачена Тарифами Банку.
1.7.4. У разі призупинення роботи Системи з будь-якої технічної причини обслуговування Клієнта здійснюється Банком з використанням Клієнтом паперових носіїв у порядку, передбаченому ДКБОФО та законодавством України.
1.7.5. Електронна платіжна інструкція вважається прийнятою Банком у випадку формування в Системі відповідного повідомлення (статусу) про прийом такої Електронної платіжної інструкції Банком. Електронні платіжні інструкції із реквізитами отримувачів за межами Банку, що надійшли до Банку до 17 год 00 хв. робочого дня, приймаються та виконуються Банком в день отримання таких Електронних платіжних інструкцій. Електронні платіжні інструкції із реквізитами отримувачів за межами Банку, що надійшли до Банку після 17 год 00 хв, робочого дня або у вихідні, неробочі чи святкові дні виконуються Банком не пізніше наступного робочого дня.
1.8. Умови користування Інформаційним режимом
1.8.1. Інформаційний режим роботи дозволяє проводити операції в Системі, не пов`язані зі зміною балансу рахунку (перегляд власних рахунків, формування виписок/реквізитів рахунків). Інформаційний режим не передбачає можливості здійснювати розрахунки у безготівковій формі та/або переказ коштів на інші рахунки. Інформаційний режим роботи доступний виключно Клієнтам, які були підключені до Системи до 01.05.2018р.
1.9. Умови користування Активним режимом
1.9.1. Активний режим дозволяє Клієнту виконувати наступні дії:

- надавати Банку доручення щодо здійснення переказів в національній валюті між власними рахунками Клієнта., зокрема:
  - ❖ перерахувати кошти з ПР/КР на ПР/КР/Вкладний Рахунок
  - ❖ погашати кредити;
  - ❖ поповнювати депозити;

- надавати Банку доручення щодо здійснення переказів в національній та/або іноземній валюті з ПР/КР на власні рахунки, відкриті у Банку - з дотриманням вимог Законодавства та режиму відповідного Рахунку;
- подавати Заявки в межах сервісу «Замовлення послуг»;
- вмикати/вимикати перевірку коду CVV2/CVC2;
- встановлювати ПІН-код по платіжним карткам;
- надавати до Банку заявку на відкриття ПР/КР/Вкладного рахунку;
- надавати до Банку заявку на підключення послуги договірного списання грошових коштів з поточного рахунку Клієнта (регулярний платіж) та закривати його;
- здійснювати інші дії передбачені ДКБОФО та Системою.

1.10. Процедура активації доступу до Системи

1.10.1. Банк здійснює реєстрацію Клієнта у Системі та надсилає пароль першого доступу до Системи у повідомленні на Фінансовий номер телефону мобільного зв'язку, що був наданий Клієнтом Банку.

1.11. Процедура автентифікації в Системі

1.11.1. Для першого входу в Систему Клієнту необхідно:

- зайти на сайт Системи https://my.bank.com.ua;
- ввести Логін та Тимчасовий пароль для входу, що надійде у вигляді повідомлення.

1.11.2. Після здійснення першого входу необхідно в обов'язковому порядку встановити постійний Пароль для Входу. Для цього необхідно ввести у відповідні поля Системи:

- пароль для Входу (свій власний пароль, який Клієнт встановлює самостійно);
- підтвердити Пароль для Входу,

1.11.3. Для наступних входів в Систему Клієнту необхідно:

- ввести Логін;
- ввести Пароль для входу (постійний пароль, який Клієнт встановив при першому вході).

1.11.4. В разі, якщо Клієнт некоректно ввів Пароль для входу Система заблокує вхід Клієнта до Системи. Кількість спроб некоректного вводу Паролю визначає Банк і вона дорівнює шести.

1.12. Поновлення Паролю для авторизації у Системі

1.12.1. Для поновлення Паролю у Системі необхідно:

- Натиснути «Забули пароль?» на стартовій сторінці/головному екрані для входу в Систему;
- На формі «Відновлення доступу» обрати «Відновити пароль»;
- Ввести логін, номер картки або номер рахунку у форматі IBAN та дату народження, перейти «далі», підтвердити дії за допомогою Разового пароля, що надійшов на Фінансовий номер телефону Клієнта;
- У разі успішного підтвердження введених даних, Клієнт отримає відповідне повідомлення, а на номер телефону буде надіслано повідомлення з тимчасовим Паролем;
- Після успішного входу в Систему з Тимчасовим паролем, необхідно встановити Пароль для входу, який буде використовуватись в майбутньому на постійній основі при кожному вході в Систему.

1.12.2. У випадку виникнення труднощів при самостійному відновленні Пароля у Системі, або якщо обліковий запис Клієнта було заблоковано з причини вводу неправильного паролю Клієнт може звернутись до відділення або ЦЕНТРУ КЛІЄНТСЬКОЇ ПІДТРИМКИ та виконати наступні дії:

- пройти ідентифікацію/автентифікацію згідно процедури та повідомити, що Пароль для авторизації в Системі необхідно поновити.

1.12.3. В разі успішної ідентифікації оператор ЦЕНТРУ КЛІЄНТСЬКОЇ ПІДТРИМКИ ініціює відправлення Тимчасового Пароля на Фінансовий номер телефону Клієнта**,** та розблокує можливість для входу Клієнтом. Після цього Клієнту необхідно зайти в Систему та здійснити процедуру першого входу, а саме:

- ввести Логін та Тимчасовий пароль для входу, що надійде у вигляді повідомлення;
- встановити Пароль для входу, який буде використовуватись в майбутньому на постійній основі при кожному вході в Систему.

1.13. Блокування доступу до Системи

1.13.1. Блокування/ відключення доступу до Системи може бути здійснено за ініціативою Клієнта, зокрема в разі якщо Клієнт не бажає користуватись Системою та/або в разі підозри Клієнта стосовно того, що його Логін та/або Пароль було скомпрометовано або його комп`ютер було інфіковано вірусами тощо. Відповідальність за збереження Логіну та Паролю покладається виключно на Клієнта. Для тимчасового блокування облікового запису, Клієнт має право звернутись до ЦЕНТРУ КЛІЄНТСЬКОЇ ПІДТРИМКИ або у відділення Банку.

1.13.2. Блокування/ відключення доступу до Системи може бути здійснено за ініціативою Банку, зокрема з метою попередження можливого шахрайства, будь-яких незаконних або непогоджених дій, що можуть призвести до фінансових збитків Банку або до погіршення іміджу Банку, у випадку закриття всіх рахунків Клієнта та розірвання всіх договорів, а також в інших випадках.

1.14. Розблокування доступу до Системи

1.14.1. Розблокування доступу до Системи, який раніше було заблоковано з ініціативи Клієнта, можливе при зверненні Клієнта до ЦЕНТРУ КЛІЄНТСЬКОЇ ПІДТРИМКИ або у відділення Банку.

1.14.2. Розблокування доступу до Системи, який раніше було заблоковано Банком у зв'язку з заміною SIM картки, можливе при зверненні Клієнта до ЦЕНТРУ КЛІЄНТСЬКОЇ ПІДТРИМКИ та після проходження стандартної та поглибленої ідентифікації Клієнта. Клієнт надає код авторизації по операції/запиту за власною платіжною карткою в АТМ або POS в касі банку, що була проведена з введенням ПІН-коду, за винятком операцій з використанням токену, що має бути здійснена

протягом 24 годин з моменту першого звернення Клієнта до ЦЕНТРУ КЛІЄНТСЬКОЇ ПІДТРИМКИ. Якщо код вірний, то працівники ЦЕНТРУ КЛІЄНТСЬКОЇ ПІДТРИМКИ розблоковують запис.

1.15. Правила виконання банківських операцій в Системі.

1.15.1. В Системі передбачена можливість здійснювати наступні види переказів в національній валюті:

- переказ коштів між власними рахунками Клієнта в Банку (тип переказу «Перекази між своїми рахунками»);
- перекази постачальникам послуг (організаціям) в межах сервісу «Оплата рахунків»;
- інші перекази.

1.15.2. З метою ініціювання переказу між власними рахунками Клієнт має здійснити наступні дії в Системі:

- вибрати пункт меню **Платежі /Створити платіж**;
- зі списку, доступного в полі **З рахунку /З карти**, вибрати той рахунок, з якого буде здійснено переказ коштів. Після того, як буде вибрано рахунок зі списку, значення поля **Доступний залишок** заповниться автоматично. В полі **З рахунку/З карти** доступний список тих рахунків, на які у Клієнта є право дебету;
- вибрати **Тип переказу - Переказ між своїми рахунками;**
- в полі **На рахунок зі списку** вибрати свій рахунок, на який будуть переказані кошти.

1.15.3. Банк виконує ініційоване Клієнтом Доручення на договірне списання з власного рахунку на інший власний рахунок (переказ) Клієнта за наступних умов:

- попередньо була успішно проведена автентифікація Клієнта в Системі;
- рахунок списання є активним, не заблокованим, не закритим;
- рахунок списання має хоча б одну активну платіжну картку (в разі, якщо рахунок списання - КР);
- рахунок зарахування є активним, не заблокованим, не закритим;
- рахунок зарахування має хоча б одну активну платіжну картку (в разі, якщо рахунок зарахування - КР);
- рахунок зарахування передбачає можливість поповнення (для вкладних рахунків);
- на рахунку списання/ балансі платіжної картки (для КР) на момент ініціювання операції достатньо коштів для здійснення переказу із врахуванням суми комісії (в разі наявності комісії за операцію згідно Тарифів);
- валюта рахунку списання співпадає із валютою рахунку зарахування;
- сума операції не перевищує встановлені Ліміти в Системі, а у разі виконання переказу з КР, - ліміти на здійснення видаткових операцій по КР з використанням платіжної картки;
- одноразовий пароль, що був введений Клієнтом, є вірним.

1.15.4. Банк виконує ініційоване Клієнтом Доручення на договірне списання з власного рахунку Клієнта на користь третьої особи (платіж) за наступних умов:

- попередньо була успішно проведена автентифікація Клієнта в Системі;
- рахунок списання є активним, не заблокованим, не закритим;
- рахунок списання має хоча б одну активну платіжну картку (в разі, якщо рахунок списання - КР);
- рахунок зарахування є активним, не заблокованим, не закритим;
- рахунок зарахування має хоча б одну активну платіжну картку (в разі, якщо рахунок зарахування - КР);
- рахунок зарахування передбачає можливість поповнення (для вкладних рахунків);
- рахунок зарахування є балансовим рахунком, на який законодавством та/або Банком не заборонено виконувати зарахування коштів;
- на рахунку списання/ балансі платіжної картки (для КР) на момент ініціювання операції достатньо коштів для здійснення платежу із врахуванням суми комісії (в разі наявності комісії за операцію згідно Тарифів);
- валюта рахунку списання та валюта рахунку зарахування - національна валюта України;
- сума операції не перевищує встановлені ліміти в Системі, а у разі виконання переказу з КР, -ліміти на здійснення видаткових операцій по КР;
- одноразовий пароль, що був введений Клієнтом, є вірним.

1.15.5. Банк виконує ініційоване Клієнтом Доручення на договірне списання з рахунку Клієнта на рахунки, відкриті в інших банках України за наступних умов:

- попередньо була успішно проведена автентифікація Клієнта в Системі;
- рахунок списання є активним, не заблокованим, не закритим;
- рахунок списання має хоча б одну активну платіжну картку (в разі, якщо рахунок списання - КР);
- рахунок зарахування є активним, не заблокованим, не закритим;
- рахунок зарахування є балансовим рахунком, на який законодавством та/або Банком не заборонено виконувати зарахування коштів;
- на рахунку списання/ балансі платіжної картки (для КР) на момент ініціювання операції достатньо коштів для здійснення платежу із врахуванням суми комісії (в разі наявності комісії за операцію згідно Тарифів);
- валюта рахунку списання та валюта рахунку зарахування - національна валюта України;
- сума операції не перевищує встановлені ліміти в Системі, а у разі виконання переказу з КР, -ліміти на здійснення видаткових операцій по КР, встановлені договором про відкриття та ведення рахунку;
- одноразовий пароль, що був введений Клієнтом, є вірним.

1.15.6. Банк виконує ініційоване Клієнтом Доручення на переказ з рахунку Клієнта на КР інших клієнтів Банку за наступних умов:

- попередньо була успішно проведена автентифікація Клієнта в Системі;
- рахунок списання є активним, не заблокованим, не закритим;
- рахунок списання має хоча б одну активну платіжну картку (в разі, якщо рахунок списання - КР);

- рахунок зарахування є активним, не заблокованим, не закритим;
- рахунок зарахування має хоча б одну активну платіжну картку;
- платіжна картка, відкрита до КР, на який здійснюється перерахування коштів, емітована Банком та є активною;
- на рахунку списання/ балансі платіжної картки (для КР) на момент ініціювання операції достатньо коштів для здійснення платежу із врахуванням суми комісії (в разі наявності комісії за операцію згідно Тарифів);
- валюта рахунку списання та валюта рахунку зарахування - національна валюта України;
- сума операції не перевищує встановлені ліміти в Системі, а у разі виконання переказу з КР - ліміти на здійснення видаткових операцій по КР, встановлені договором про відкриття та ведення рахунку;
- одноразовий пароль, що був введений Клієнтом, є вірним.

1.15.7. В межах сервісу «Оплата рахунків» Клієнт може обрати постачальника послуг (організацію) та здійснити переказ на його користь. Для цього Клієнт має виконати наступні дії:

- вибрати пункт меню **Оплата рахунків/Сплатити рахунок;**
- виконати пошук постачальника послуг (організації), рахунок якого планує сплатити;
- заповнити реквізити, потрібні для сплати рахунку;
- ввести суму переказу, натиснути кнопку «Далі»;
- зі списку, доступного в полі **З рахунку /З карти**, вибрати рахунок або картку, з якого/ї буде здійснено переказ коштів.
- в полі **З рахунку/З карти** доступний список тих рахунків, на які у Клієнта є право дебету;
- на наступній сторінці необхідно перевірити правильність заповнення реквізитів. Якщо дані помилкові, натиснути кнопку «Повернутися/Назад» і виправити їх, якщо вірні – підписати документ за допомогою разового паролю;

якщо документ був успішно відправлений в Банк, на екрані з'явиться відповідне повідомлення.

1.15.8. Заява Клієнта про повернення коштів у разі невдалої сплати в межах сервісу «Оплата рахунків» на користь постачальника послуги (організації) приймається до розгляду за умови, якщо статус переказу в Системі «Відхилений», кошти були списані та не повернулися на рахунок Клієнта автоматично в поточному та наступному робочому дні, або статус переказу в Системі дистанційного обслуговування «ПІВДЕННИЙ MYBANK» «Проведений», але кошти не дійшли на рахунок постачальника послуги (організації). Клієнт може подати Заяву на повернення коштів, звернувшись до відділення Банку або ЦЕНТРУ КЛІЄНТСЬКОЇ ПІДТРИМКИ, або подавши дистанційну заявку в межах сервісу "Замовлення послуг".
Заява розглядається Банком протягом 30 днів з моменту реєстрації заяви в Банку. Після розгляду Заяви Банк повертає кошти на рахунок Клієнта, або надає письмову відповідь Клієнту про неможливість повернення коштів, у разі коректності та успішності проведеної операції та зарахування коштів на користь постачальника послуги (організації).

1.15.9. Перед початком надання Банку доручення щодо здійснення переказу коштів Клієнт повинен ознайомитись з встановленими Банком Лімітами в Системі, які зазначені в Системі у Розділі Налаштування/Ліміти. Ліміти встановлюються Банком для переказів типу «Переказ на карту іншого клієнта банку», «Внутрішньобанківський переказ» і «Переказ по Україні», "Оплата рахунків" на суму однієї операції, та/або на суму операцій за операційний день, та/або на суму операцій за календарний місяць та можуть бути змінені Банком. Клієнт має право на встановлення індивідуального ліміту звернувшись до відділення Банку або ЦЕНТРУ КЛІЄНТСЬКОЇ ПІДТРИМКИ, або подавши дистанційну заявку в межах сервісу «Замовлення послуг». В межах сервісу "Оплата рахунків" індивідуальні ліміти не встановлюються.

1.15.10. В Системі дистанційного обслуговування «ПІВДЕННИЙ MYBANK» Платник має право відкликати згоду на виконання платіжної операції до моменту введення всіх необхідних реквізитів для проведення операції (шляхом припинення введення інформації) та підписання платіжної інструкції. З моменту підписання платіжної інструкції та направлення її до Банку платіжна операція є безвідкличною.

1.16. Подання онлайн-заявки на відкриття вкладу (депозиту)

1.16.1. Для подання онлайн-заявки на відкриття вкладу (депозиту) (онлайн-заявка), Клієнт має здійснити наступні дії в Системі: вибрати пункт меню **Депозити /Новий депозит.** При переході на сторінку з оформлення депозиту, Клієнт має заповнити наступну інформацію:

- «Розмістити з рахунку» -вибрати рахунок (лише власні рахунки Клієнта), з якого будуть залучатися кошти на поповнення депозиту у відповідній валюті. **Увага!** Рахунок, з якого буде залучатися депозит, - це завжди рахунок, на який буде повернуто депозит по закінченню терміну договору;
- «Виберіть тип депозиту» - вибрати необхідний тип депозиту у відповідній валюті;
- «Строк депозиту» - вибрати необхідний строк депозиту, що передбачено умовами відповідної депозитної моделі;
- «Сума депозиту» - вказати суму депозиту;
- «Рахунок для зарахування %%» - вибрати рахунок, на який буде здійснюватися зарахування відсотків по депозиту.

- В разі, якщо параметри депозиту відповідають вимогам Клієнта, необхідно натиснути кнопку «Далі» , після чого Клієнт переходить на сторінку з описом «Параметрів відкриття депозиту», де має можливість ознайомитися з параметрами раніше вибраного депозитного продукту. Натиснувши кнопку «Підписати(SMS)» Клієнт автоматично направляється на сторінку «Заявка на відкриття депозиту», де необхідно ввести код підтвердження із SMS. Після зазначених дій, заявка на відкриття депозиту буде відправлена на опрацювання в Банк.

Клієнт має можливість переглянути створені онлайн-заявки на відкриття вкладів (депозитів) і їх статуси. Список онлайн-заявок можна переглянути у розділі Депозити/Список заявок.

1.16.2. Також, онлайн-заявку на відкриття вкладу (депозиту) можна подати до Банку одразу, без заповнення форми «Підібрати і відкрити», шляхом заповнення відповідної заявки у розділі Депозити/Новий депозит/Відкрити депозит.

1.17. Подання розпорядження на встановлення регулярного платежу

Для подання розпорядження на встановлення регулярного платежу, Клієнт має здійснити наступні дії:

- вибрати пункт меню **Платежі/Регулярні платежі та натиснути кнопку «Створити платіж»**
- заповнити обов’язкові параметри регулярного платежу, а саме:

- найменування Регулярного платежу;
- з рахунку – вибрати рахунок, з якого Клієнт бажає встановити регулярний платіж;
- тип переказу – вибрати зі списку тип переказу;
- реквізити отримувача – код банку, номер рахунку одержувача, найменування одержувача, РНОКПП/ЄДРПОУ;
- реквізити переказу – сума переказу, періодичність, призначення платежу.

- після заповнення всіх обов'язкових параметрів регулярного платежу, необхідно натиснути кнопку «Далі»;
- на сторінці «Попередній перегляд платежу», Клієнт має можливість перевірити коректність заповнення форми на встановлення регулярного платежу, після чого необхідно натиснути кнопку «Підписати(SMS)»;
- Клієнт переходить на сторінку «Регулярний платіж», де необхідно ввести код підтвердження із SMS. Після зазначених дій, заявка на встановлення регулярного платежу буде відправлена на опрацювання в Банк. Клієнт має можливість переглянути створені розпорядження на встановлення регулярних платежів і їх статуси. Список розпоряджень на встановлення регулярних платежів можна переглянути у розділі **Платежі/Регулярні платежі/Список регулярних платежів.** Прийом на виконання нових розпоряджень на встановлення регулярного платежу відбувається в Банку протягом операційного часу. Розпорядження на встановлення регулярного платежу, які були створені після операційного часу, будуть прийняті Банком протягом операційного часу наступного робочого дня. Виконання регулярного платежу для типу переказу «з картки на картку» та «на картку іншого клієнта банка» відбувається щодня, для усіх інших типів переказів виконання Регулярного платежу відбувається у робочі дні згідно умов ДКБОФО. У випадку невдалого виконання регулярного платежу, наприклад, у разі відсутності коштів на рахунку Клієнта, система виконає ще дві спроби на виконання цього платежу протягом операційного часу Банку.
- У разі необхідності припинити дію Регулярного платіжу, Клієнт переходить на детальну форму Регулярного платежу та натискає «Закрити» та підтверджує свою дію. На формі Списку регулярних платежів Клієнт має можливість стежити за статусом Регулярного платежу, який зміниться на «Закритий».

1.18. Подання дистанційних заявок на замовлення продуктів та послуг (далі - Заявка) в межах сервісу «Замовлення послуг» в Системі дистанційного обслуговування «ПІВДЕННИЙ MYBANK»

У Системі дистанційного обслуговування «ПІВДЕННИЙ MYBANK» можуть бути оформлені зокрема, але не винятково такі заявки:

- заява-договір банківського рахунку з використанням ПК;
- заява на переоформлення платіжної картки;
- заява на оформлення додаткової платіжної картки;
- заява на повернення коштів;
- заява на зміну лімітів;
- заява на надання реквізитів ПР/КР;
- заява на уточнення реквізитів платіжу;
- заява на зміну рахунку–кореспондента;
- заява на закриття ПР/КР;
- заява на встановлення/зміну кодового слова Клієнта;
- заява на отримання довідок клієнтами- фізичними особами;
- заява на продовження дії договору оренди індивідуального банківського сейфу;
- заява на одноразове відвідування сейфу для вилучення цінностей;
- заява на перерахування коштів, що гарантуються Фондом гарантування вкладів фізичних осіб;
- заява на зміну фактичної адреси проживання;
- заява на оновлення ідентифікаційних даних;
- заява на переказ валюти на рахунок родича в межах Банку;
- заява на доставку ПК по Україні.

Для подання заявки на замовлення певних продуктів та послуг в Банку, Клієнт має здійснити наступні дії в Системі:

- вибрати пункт меню **Замовлення послуг/ натиснути кнопку «Створити заявку»;**
- обрати потрібний пункт в розділі «Продукт/послуга» з переліку доступних та тип заявки в розділі «Деталі»;
- заповнити Заявку;
- перевірити коректність заповнення форми та натиснути «Підписати(SMS)»;
- Клієнт переходить на наступну сторінку «Замовлення продуктів та послуг», де необхідно ввести код підтвердження із SMS. Після зазначених дій, Заявка буде відправлена на опрацювання до Банку;
- Клієнт має запевнитись, що операція підтвердження Заявки пройшла успішно та Заявка має статус «Введений» у переліку Заявок.

Заявки на замовлення продуктів та послуг розглядаються Банком протягом трьох робочих днів. У разі неможливості виконати Заявку Клієнта Банк відхиляє заявку у Системі та Клієнт може побачити її статус «Відхилений» та причину відхилення та/або Банк може повідомити про це Клієнта за телефоном, шляхом надсилання повідомлення або повідомлення в Системі.

1.19. Заходи безпеки при користуванні Системою

1.19.1. Для отримання доступу до Системи Клієнт зобов'язаний використовувати персональний комп'ютер або інший пристрій, що забезпечує доступ до мережі Інтернет та на який встановлено:

- операційну систему (наприклад, Microsoft Windows) з останніми оновленнями;
- останню доступну версію браузера;
- ліцензійне антивірусне програмне забезпечення з останніми оновленнями баз вірусних сигнатур;

- антишпигунське програмне забезпечення (antispyware) та програмний персональний мережевий екран (firewall) з останніми оновленнями.

1.19.2. Рекомендується регулярно (не рідше, ніж раз на тиждень) здійснювати повне сканування персонального комп'ютера (іншого пристрою) для виявлення вірусів та зловмисного програмного забезпечення.

1.19.3. Не рекомендується встановлювати на персональний комп'ютер (інший пристрій) програмне забезпечення із ненадійних джерел (публічні бібліотеки програмного забезпечення, програми в електронних повідомленнях тощо).

1.19.4. Дані з автентифікації повинні зберігатися в таємниці, а мобільний телефон (SIM-карта, що відповідає Фінансовому номеру телефону Клієнта) – під постійним особистим контролем Клієнта. При використанні даних з автентифікації необхідно:

- Логін та Пароль зберігати окремо.
- перед зміною Паролю, перевірити сертифікат безпеки банківського сервера.

1.19.5. Політика паролів:

- паролі повинні бути унікальні для кожного Клієнта даного робочого місця протягом усього часу роботи системи, містити тільки латинські букви різних регістрів, цифри і допустимі символи:! @ # $% * () _ - + = |. Усі інші символи, пробіл та інші мови (не латинські) є недопустимими. Пароль для входу в Систему не повинен містити словарне значення або ім'я, пов'язане з користувачем (ім'я, прізвище, ім'я дружини, дітей тощо), не містити послідовності знаків, що повторюються (наприклад, «access»), очевидних послідовностей та узорів, які створюються символами, нанесеними на клавіші клавіатури (наприклад, qwert або zxcvb). Пароль повинен бути довжиною не менше 8 символів і задовольняти вимогам по його складності тобто одночасно містити як великі, так і маленькі букви, цифри. Пароль та Логін Клієнта не можуть співпадати.
- при зміні пароля він не повинен повторювати 5 останніх Паролів.
- термін дії Пароля не може перевищувати 365 днів від дати встановлення постійного Пароля. Зміна Пароля відбувається при вході в Систему згідно з вимогами безпеки систем обслуговування клієнтів Банку.
- в розділі «Налаштування» в Системі Клієнт може самостійно встановити термін у кількості днів для повідомлення його про необхідність зміни Пароля. Установче налаштування терміну повідомлення Клієнта про необхідність зміни Пароля сім днів.

1.19.6. При використанні Системи Клієнт повинен:

- здійснювати підключення до Системи тільки з надійних робочих станцій, уникати підключення з публічних місць (Інтернет-кафе, готелів, бібліотек тощо);
- впевнитись при вході в Систему дистанційного обслуговування «ПІВДЕННИЙ MYBANK», що в адресному полі браузера знаходиться адреса саме Системи дистанційного обслуговування «ПІВДЕННИЙ MYBANK»;
- перевіряти надійність надавача сертифікату, дійсність сертифікату та термін його дії. Підтвердженням того, що між браузером Клієнта та сервером Банку встановлено безпечне з'єднання, є наявність цифрового (електронного) сертифікату Банку;
- не залишати персональний комп'ютер (інший пристрій, з якого здійснюється доступ до Системи) без нагляду;
- закінчувати поточну сесію (тобто, закінчувати роботу з Системою) через посилання Вихід та закривати вікно браузера;
- якщо вхід у Систему здійснюється в публічних місцях, перед закриттям вікна браузера очистити буфер браузера та видалити тимчасові файли та cookies;
- не переглядати інші сайти в тому ж браузері, коли Клієнт працює в Системі;
- стежити за тривалістю сесії (тривалості знаходження в Системі без будь-яких дій з боку Клієнта), яка задля безпеки обмежена 10 хвилинами;
- для навігації в Системі використовувати виключно посилання і кнопки Системи та не використовувати кнопки навігації браузера (наприклад Вперед/Назад);
- звертати увагу на повідомлення браузера про небезпеку.

1.19.7. При використанні Системи Клієнту забороняється:

- переходити до стартової сторінки Системи за банерним посиланням або посиланнями, отриманими електронною поштою;
- відповідати на запити (найчастіше розсилаються електронною поштою), які містять вимогу надати або перевірити Логін, Пароль для входу та/або інші дані автентифікації.

1.19.8. Банк за жодних обставин не здійснює:

- розсилку електронних листів із вимогою надіслати Пароль для входу, Логін та/або інші дані автентифікації та/або не пропонує перейти за вказаною електронною адресою.
- розповсюдження електронною поштою комп'ютерних програм.

1.19.9. Рекомендується видаляти підозрілі електронні листи без їх відкриття, особливо листи від невідомих відправників із прикріпленими файлами, що мають розширення *.exe, *.pif, *.vbs та інші файли.

1.19.10. У разі виявлення будь-якого зловмисного програмного забезпечення (віруси, троянські програми тощо) на робочій станції, необхідно здійснити вхід в Систему із гарантовано незараженої робочої станції та замінити пароль доступу до Системи.

1.19.11. При виявленні спроби несанкціонованого доступу до Системи необхідно терміново змінити Пароль для входу до Системи та звернутися до ЦЕНТРУ КЛІЄНТСЬКОЇ ПІДТРИМКИ для блокування доступу до Системи. Рекомендується також провести сканування робочої станції на виявлення вірусів та іншого зловмисного програмного забезпечення.

1.19.12. Установлення ПІН-коду в Системі дистанційного обслуговування «ПІВДЕННИЙ MYBANK» здійснюється на детальній формі ПК шляхом введення нового ПІН-коду. Першою операцією для ПК з чипом після установлення ПІН-коду в Системі дистанційного обслуговування «ПІВДЕННИЙ MYBANK» має бути операція по ПК (перевірка балансу ПК або видача готівки), що проводиться із введенням нового ПІН-коду в банкоматі або платіжному терміналі у відділенні Банку.

1.20. Умови подання Клієнтом Дистанційного розпорядження на обмін валют в Системі дистанційного обслуговування «ПІВДЕННИЙ MYBANK» та порядок його виконання Банком:

1.20.1. Клієнт може надати Банку Дистанційне розпорядження на обмін валюти в Системи дистанційного обслуговування «ПІВДЕННИЙ MYBANK», для цього Клієнт заповнює Заявку на купівлю, продаж або конвертацію валюти обравши необхідний пункт меню в розділі «Обмін валют» в Системі;

1.20.2. Клієнт отримує детальну інформацію щодо переліку доступних валютних пар, курсів та лімітів та обмежень обміну валют (за наявності) безпосередньо при створенні Дистанційного розпорядження на обмін валюти в розділі «Обмін валют» в Системі;

1.20.3. Клієнт може відкликати Дистанційне розпорядження на обмін валюти після його введення, натиснувши кнопку «Повернутися», якщо Клієнтом не був введений одноразовий пароль;

1.20.4. Банк на власний розсуд:

- встановлює та змінює Курс Дистанційного обміну валют протягом дня;
- встановлює регламент роботи Дистанційного обміну валют
- визначає доступні операції (купівля/продаж/конвертація) та валютні пари для Дистанційного обміну валют;
- може обмежити право Клієнта купувати валюту за рахунок Кредитного ліміту;
- може встановлювати мінімальну /максимальну суму операції для Дистанційного розпорядження на обмін валют;
- може обмежувати загальну суму купівлі валюти в еквіваленті за офіційним курсом гривні до іноземних валют, установленим Національним банком на дату здійснення операції Клієнтом протягом дня та/або місяця.

1.20.5. Комісія за послугу Дистанційного обміну валют Банком не стягується. Проте, Банком може стягуватися комісія за умови купівлі іноземної валюти за рахунок кредитних коштів (кредитного ліміту), що визначена умовами обслуговування такого рахунку та Тарифами.

1.20.6. Банк інформує Клієнта про успішність/неуспішність виконання Дистанційного розпорядження на обмін валют за допомогою відповідного повідомлення, а також надає Клієнту можливість самостійно перевірити статус Дистанційного розпорядження на обмін валют та його деталі у Системі, зокрема, курс, за яким була здійснена валютна операція.

1.20.7. Банк повертає Дистанційне розпорядження на обмін валюти без виконання у разі:

- недостатності коштів на поточному рахунку та ПК Клієнта на момент виконання розпорядження Банком;
- якщо курс Банку для Дистанційного обміну валют змінився на момент прийняття Банком на обробку Дистанційного розпорядження на обмін валюти;

1.20.8. Створення Дистанційного розпорядження на обмін валют можливе за наявності у Клієнта поточних рахунків для списання та зарахування коштів у національній валюті та/або іноземних валютах залежно від типу операції та необхідної для неї валютної пари.

1.21. Клієнт зобов'язується:

• не підключатись до Системи дистанційного обслуговування «ПІВДЕННИЙ MYBANK» через Wi-Fi-точки публічного доступу, які не потребують ідентифікації під час підключення (введення для підключення персонального імені та пароля);

• не встановлювати на телефон/пристрій, який використовується для підключення до Системи дистанційного обслуговування «ПІВДЕННИЙ MYBANK», неліцензійних операційних систем, оскільки це відключає захисні механізми, закладені виробником мобільної платформи;

• для виключення несанкціонованого використання послуг Системи дистанційного обслуговування «ПІВДЕННИЙ MYBANK» не залишати свій телефон/пристрій, який використовується для підключення до Системи дистанційного обслуговування «ПІВДЕННИЙ MYBANK», без нагляду.

2. ПРАВИЛА КОРИСТУВАННЯ МОБІЛЬНИМ ЗАСТОСУНКОМ «PIVDENNY ONLINE»

2.1. Банк надає Клієнту послуги обслуговування у Застосунку шляхом здійснення Клієнтом самостійної реєстрації відповідно до умов **ДКБОФО** та за умови наявності у Клієнта відкритого КР та активної картки або проходження Клієнтом процедури онлайн реєстрації нового користувача.

Мобільний застосунок «PIVDENNY ONLINE» може використовуватися для підписання Електронних документів (у тому числі Електронних договорів), здійснення Договірного списання коштів з Рахунків Клієнта в Банку, а також надання інших послуг, передбачених ДКБОФО та функціоналом Застосунку.

Перелік та доступність послуг, які Клієнт може отримати за допомогою Застосунку, їх зміст та порядок надання їх Клієнту, порядок роботи Застосунку можуть змінюватися в залежності від зміни функціональних можливостей Застосунку.

Підключення та надання доступу до Мобільного застосунку «PIVDENNY ONLINE» Клієнтам-фізичним особам здійснюється Банком виключно Клієнту. Підключення та надання доступу до Мобільного Застосунку «PIVDENNY ONLINE» представникам Клієнта, а також малолітнім та неповнолітнім особам забороняється.

2.2. Мобільний застосунок «PIVDENNY ONLINE» може використовуватися з метою дистанційної ідентифікації та верифікації особи Клієнта за умови проходження Клієнтом процедури онлайн реєстрації нового користувача.

2.2.1. Для проходження процедури онлайн реєстрації нового користувача, Клієнт має:

- вказати мобільний номер телефону та підтвердити його одноразовим паролем (OTP);
- мати е-паспорт/е-паспорт для виїзду за кордон у мобільному застосунку «Дія» та надати відповідний дозвіл на передачу документів в Банк для проведення належної перевірки Клієнта;
- заповнити необхідну інформацію на екранних формах Мобільного застосунку «PIVDENNY ONLINE» (зокрема Опитувальний лист Клієнта - фізичної особи, Документ самостійної оцінки);
- ознайомитися із сформованими електронними документами, необхідними для проведення належної перевірки/належної комплексної перевірки Клієнта, та надання відповідної Банківської послуги, а також акцептувати електронні документи підписом за допомогою сервісу «Дія.Підпис» через мобільний застосунок «Дія».

2.2.2. Банк, на основі інформації, поданої Клієнтом, приймає рішення про дистанційне встановлення ділових відносин/ оформлення Заяви-Договору про надання банківського продукту/послуги, про що сповіщає Клієнта через PUSH-сповіщення у Мобільному застосунку «PIVDENNY ONLINE», якщо Клієнт надав відповідний дозвіл або шляхом SMS-повідомлення чи Viber на мобільний номер телефону Клієнта, зазначений Клієнтом в процесі онлайн реєстрації.
2.2.3. Для завершення процесу онлайн реєстрації Клієнту необхідно встановити пароль для входу до Застосунку.
2.3. За наявності активної картки Банку, Клієнт має можливість здійснити процедуру самостійної реєстрації у Мобільному застосунку «PIVDENNY ONLINE». Для цього Клієнту необхідно ввести фінансовий або основний номер телефону, який Клієнт вказав як основний під час оформлення Заяви-Договору про надання банківського продукту/послуги, підтвердити номер телефону одноразовим паролем (OTP), який надсилається системою на наданий Клієнтом номер телефона, ввести/відсканувати/зчитати реквізити активної ПК Банку (номер картки, термін дії (допускається введення терміну дії простроченої картки починаючи з 02/2022) та PIN-код платіжної карти), встановити пароль для входу до Застосунку.
2.4. Після реєстрації та встановлення паролю Клієнт може додатково встановити вхід до Мобільного Застосунку «PIVDENNY ONLINE» за допомогою PIN-коду доступу або біометрії (FingerPrint/Face ID).
2.5. Надання Послуг у Застосунку здійснюється Банком у відповідності до Тарифів, чинних на момент проведення відповідної операції.
2.6. Під час першого входу до Застосунку та при доступності нового функціоналу в Застосунку відображаються екрани з повідомленням про доступний функціонал та принципи його роботи.

2.7. Робота Застосунку

2.7.1. Клієнт отримує можливість обслуговуватись у Застосунку в обсязі, визначеному Банком, з урахуванням режимів Рахунків і законодавства України, з моменту успішної автентифікації у Застосунку Клієнта. Для реєстрації та автентифікації в Застосунку Клієнт має здійснити відповідні дії, що визначені та регламентуються цими Правилами.
2.7.2. Якщо особа використала Логін та Пароль для доступу до Застосунку (в томи числі за допомогою Технології FingerPrint/Face ID/ PIN-коду доступу), та/або Разовий пароль – для здійснення операції у Застосунку, Банк безумовно вважає таку особу Клієнтом і не несе відповідальності за дії такої особи, якщо такі дії будуть оскаржуватись Клієнтом.
2.7.3. Банк зобов'язується виконувати доручення Клієнта про здійснення операцій за Рахунками, підтверджені Разовим паролем (за виключенням випадків з обмеженням розпорядження коштами відповідно до законодавства), за умови наявності коштів на Рахунках та коштів для сплати винагороди Банку за надання послуг, оплата яких передбачена Тарифами Банку.
2.7.4. Електронні платіжні інструкції, що надсилаються Клієнтом за допомогою Застосунку, повинні бути оформлені Клієнтом відповідно до вимог Законодавства України, в тому числі, нормативно-правових актів Національного банку України, та за умови підтвердження Разового пароля. При цьому, коли Клієнт вводить Разовий пароль, Клієнт підтверджує, що він ознайомлений з умовами, на яких здійснюється платіж, в тому числі з Тарифами Банку, та погоджується з ними.
2.7.5. Електронні інформаційні документи (листи, розпорядження) повинні бути оформлені Клієнтом належним чином та підтверджені Разовим паролем.
2.7.6. У разі призупинення роботи Застосунку з будь-якої технічної причини обслуговування Клієнта здійснюється Банком з використанням Клієнтом паперових носіїв у порядку, передбаченому ДКБОФО та законодавством України.
2.7.7. Електронні платіжні інструкції вважаються прийнятими Банком у випадку формування в Застосунку відповідного повідомлення (статусу) про прийом такого Електронного платіжного документу Банком. Електронні платіжні інструкції із реквізитами отримувачів за межами Банку, що надійшли до Банку до 17 год 00 хв. робочого дня, приймаються та виконуються Банком в день отримання таких Електронних платіжних інструкцій. Електронні платіжні інструкції із реквізитами отримувачів за межами Банку, що надійшли до Банку після 17 год 00 хв, робочого дня або у вихідні, неробочі та святкові дні виконуються Банком не пізніше наступного робочого дня.
2.7.8. У мобільному застосунку «PIVDENNY ONLINE» перед виконанням платіжної операції Клієнту надається можливість протягом встановленого Банком періоду очікування підтвердити виконання операції або скасувати її, у разі:

- підтвердження Клієнтом виконання операції — мобільний застосунок «PIVDENNY ONLINE», негайно переходить до етапу виконання платіжної операції;
- скасування Клієнтом операції — платіжна інструкція не передається Банку до виконання та операція припиняється;
- відсутності дій Клієнтом протягом встановленого періоду очікування — мобільний застосунок «PIVDENNY ONLINE» автоматично переходить до етапу виконання платіжної операції.

Після надання Клієнтом згоди на виконання платіжної операції Банк приймає платіжну операцію до виконання. З цього моменту така платіжна інструкція вважається безвідкличною, а Клієнт не має права відкликати або змінити її.

2.8. Умови користування Застосунком

2.8.1. Застосунок дозволяє Клієнту виконувати зокрема, але не виключно, наступні дії:

- надавати Банку платіжні інструкції щодо здійснення переказів в національній та/або іноземній валюті з ПР та своєї ПК на власні ПР та ПК відкриті у Банку - з дотриманням вимог Законодавства та режиму відповідного Рахунку;
- надавати Банку платіжні інструкції щодо здійснення переказів в національній валюті з ПР/КР/ПК Клієнта на ПК іншого банку України (крім операцій з перерахування коштів із ПР/КР/ПК Клієнтів - резидентів на ПР/КР/ПК Клієнтів-нерезидентів);
- надавати Банку платіжні інструкції щодо здійснення переказів в національній валюті з ПК Клієнта в іншому банку України на ПК Клієнта в Банку;
- надавати Банку платіжні інструкції на здійснення переказів в національній валюті з КР на рахунки юридичних осіб, відкриті у Банку та в інших банках на території України;
- надавати Банку платіжні інструкції на здійснення переказів в національній валюті з КР/ПК на КР/ПК інших фізичних осіб, відкриті у Банку та/або на КР/ПК інших фізичних осіб відкритих в інших банках на території України;

- перекази здійснюються в межах лімітів, встановлених Банком, з дотриманням вимог законодавства та режиму відповідного рахунку;
- здійснювати поповнення балансу мобільного телефону українських мобільних операторів;
- здійснювати операції Дистанційного обміну валют;
- здійснювати випуск ПК до існуючого поточного рахунку з використанням електронних платіжних засобів, у т.ч. віртуальної ПК;
- встановлювати ПІН-код по ПК;
- блокувати/розблоковувати власні ПК (у випадку втрати, крадіжки, компрометації);
- додавати ПК до гаманця Apple Wallet (на пристроях з ОС iOS) та Google Pay (на пристроях з ОС Android);
- керувати системою PUSH-сповіщень;
- отримувати інформацію щодо залишку коштів на рахунках Клієнта;
- отримувати інформацію історії операцій за КР Клієнта;
- отримувати інформацію щодо реквізитів ПК Клієнта;
- активувати ПК Клієнта, що була отримана Клієнтом;
- можливість здійснити повторення платежу, що був виконаний з ПК у Застосунку;
- автоматично формувати лист з інформацією щодо роботи Застосунку та надсилати лист на e-mail ЦЕНТРУ КЛІЄНТСЬКОЇ ПІДТРИМКИ.
- отримання виписки за поточним рахунком з використанням електронних платіжних засобів;
- відкриття депозиту згідно діючої лінійки вкладів для ФО;
- поповнення депозиту (якщо умовами вкладу передбачено поповнення);
- часткове зняття коштів (якщо умовами вкладу передбачено);
- відмовитись від подальшої автоматичної пролонгації вкладу (якщо умовами вкладу передбачено);
- поновити автоматичну пролонгацію вкладу (якщо умовами вкладу передбачено);
- дострокове розірвання договору вкладу (якщо умовами вкладу передбачено);
- відображення історії операції по депозиту (поповнення, виплата процентів, зняття);
- ініціювати закриття ПР/КР;
- зберігати дані власної платіжної картки іншого банку;
- відображення кредитної карти (обов'язкового мінімального платежу, повної суми заборгованості, нарахованих процентів);
- здійснювати операції по кредитній картці з погашення обов'язкового мінімального платежу;
- здійснювати операції по кредитній картці з погашення повної суми заборгованості;
- відображення Договору оренди (параметри Договору оренди, у т.ч. відображення довірених осіб);
- відмовитись від автоматичної пролонгації строку дії Договору оренди (якщо умовами Договору оренди передбачена автоматична пролонгація);
- поновити автоматичну пролонгацію Договору оренди (якщо умовами Договору оренди спочатку була передбачена автоматична пролонгація);
- продовжити строк користування Сейфом (укладання Додаткового договору);
- надання послуги «Миттєвий платіж»; надання доступу до відкритих в Банку Рахунків Клієнта та підтвердження згоди на здійснення платежу у межах сервісу «Open Banking»;
- надання сервісу «Платежі за номером телефону».

Надання послуг у Застосунку здійснюється Банком за наявності технічної можливості.

2.9. Процедура активації доступу та перший вхід до Застосунку за умови наявності у Клієнта ПК

2.9.1. Для реєстрації у Застосунку Клієнту необхідно:

- ввести фінансовий або основний номер телефону (Логін) та підтвердити за допомогою OTP-паролю, що надсилає Банк в повідомленні на зазначений номер телефона під час реєстрації;
- ввести дані ПК Клієнта в Банку (номер карти, термін дії та PIN-код платіжної карти);
- встановити пароль для входу у Застосунок, додатково Клієнт має можливість встановити PIN-код доступу/FingerPrint/Face ID.
- пройти перевірки:
  - ❖ номер телефону та номер ПК, що підтверджено, належать одному і тому ж Клієнту Банку;
  - ❖ номер ПК та введений Клієнтом CVV2\CVC2 код до неї, коректні та ПК активна. Під час перевірки даних ПК виконується авторизація в процесинговому центрі на 0 грн. 00 коп.

2.10. Процедура автентифікації в Застосунку з активного пристрою

2.10.1. Для наступних входів у Застосунок з активного пристрою (з якого була виконана автентифікація минулого разу) Клієнту необхідно:

- ввести Логін (у Застосунку передбачено автоматичне заповнення Логіну за відповідних умов);
- ввести Пароль для входу, який встановив Клієнт або PIN-код доступу/FingerPrint/Face ID, якщо вони встановлені;
- кількість спроб некоректного вводу Паролю Клієнтом до Застосунку складає 5 спроб, після чого обліковий запис користувача блокується на 15 хвилин. При цьому, якщо у Клієнта додатково встановлено FingerPrint/Face ID або PIN-код доступу, то в такому випадку:
  - якщо встановлено FingerPrint/Face ID та Клієнт використав 5 спроб ідентифікувати особу за допомогою FingerPrint/Face ID, тоді Клієнт переадресується на сторінку входу по PIN-коду, якщо такий установлено, в іншому випадку на сторінку входу по Паролю;

- якщо встановлено PIN-код доступу та Клієнт використав 5 спроб ідентифікувати особу за допомогою PIN-коду доступу, тоді Клієнт переадресується на сторінку входу по Паролю.

2.11. Процедура автентифікації у Застосунку з нового пристрою або після виходу з Застосунку

2.11.1. Для входу з нового пристрою у Застосунок або після виконання процедури виходу із Застосунку відповідно до функціоналу Клієнту необхідно:

- ввести номер телефону (Логін) та підтвердити за допомогою ОТР паролю, що надсилає Банк в повідомленні на зазначений номер телефона;
- ввести Пароль для входу, який встановив Клієнт або PIN-код доступу/FingerPrint/Face ID, якщо вони встановлені;
- ввести дані ПК Клієнта в Банку (номер карти, термін дії та PIN-код платіжної карти);
- пройти перевірки:
  - ❖ номер телефону та номер ПК, що підтверджено, належать одному і тому ж Клієнту Банку;
  - ❖ номер ПК та введений Клієнтом PIN-код до неї, коректні та ПК активна. Під час перевірки даних ПК виконується авторизація в процесинговому центрі на 0 грн. 00 коп.

2.12. Поновлення Паролю для авторизації у Застосунку

2.12.1. Для поновлення Паролю у Застосунку Клієнту необхідно:

- натиснути «Забули пароль?» на головному екрані входу в Застосунок;
- ввести ОТР пароль, що надсилає Банк в повідомленні на фінансовий/основний номер телефону Клієнта;
- ввести дані ПК Клієнта в Банку (номер карти, термін дії та PIN-код платіжної карти);
- пройти перевірки:
  - ❖ номер телефону та номер ПК, що підтверджено, належать одному і тому ж Клієнту Банку;
  - ❖ номер ПК та введений Клієнтом CVV2\CVC2 код до неї, коректні та ПК активна. Під час перевірки даних ПК виконується авторизація в процесинговому центрі на 0 грн. 00 коп.;
- встановити новий Пароль для входу в Застосунок.

2.13. Вихід із Застосунку

2.13.1. Для виходу з облікового запису у Застосунку Клієнту необхідно вибрати відповідний функціонал «Вихід» у меню «Профіль користувача» та підтвердити свій намір за допомогою ОТР-паролю, що надсилається банком у повідомленні для підтвердження.

2.14. Блокування доступу до Застосунку

2.14.1. Блокування доступу до Застосунку може бути здійснено за ініціативою Клієнта, якщо він не бажає користуватись Застосунком та/або в разі підозри Клієнта стосовно того, що його Логін та/або Пароль було скомпрометовано. Відповідальність за збереження Логіну та Паролю покладається виключно на Клієнта. Для тимчасового блокування доступу до Застосунку, Клієнту необхідно звернутись до ЦЕНТРУ КЛІЄНТСЬКОЇ ПІДТРИМКИ або у відділення Банку.

2.14.2. Блокування доступу до Застосунку може бути здійснено за ініціативи Банку для попередження можливого шахрайства, будь-яких незаконних або непогоджених дій, що можуть призвести до фінансових збитків Банку або до погіршення його іміджу.

2.15. Розблокування доступу до Застосунку

2.15.1. Розблокування доступу до Застосунку, який раніше було заблоковано з ініціативи Клієнта, можливе при зверненні Клієнта до ЦЕНТРУ КЛІЄНТСЬКОЇ ПІДТРИМКИ або у відділення Банку.

2.15.2. Розблокування доступу до Застосунку, який раніше було заблоковано Банком у зв'язку з заміною SIM ПК, можливе при зверненні Клієнта до ЦЕНТРУ КЛІЄНТСЬКОЇ ПІДТРИМКИ та після проходження стандартної та поглибленої ідентифікації Клієнта. Клієнт надає код авторизації по операції/запиту за власною ПК в АТМ або POS в касі банку, що була проведена з введенням ПІН-коду, за винятком операцій з використанням токену, що має бути здійснена протягом 24 годин з моменту з моменту першого звернення Клієнта до ЦЕНТРУ КЛІЄНТСЬКОЇ ПІДТРИМКИ. Якщо код вірний, то працівники ЦЕНТРУ КЛІЄНТСЬКОЇ ПІДТРИМКИ розблоковують запис.

2.16. Правила виконання банківських операцій у Застосунку.

2.16.1. У Застосунку передбачена можливість здійснювати наступні види переказів у меню «Перекази», розділ «Перекази», тип переказу «На ПК або рахунок»:

- переказ з ПК Клієнта на ПК іншого банку України;
- переказ з ПК іншого банку України на ПК Клієнта;
- переказ з ПК Клієнта на ПК іншого клієнта Банку;
- переказ між ПК Клієнта;
- переказ з ПК Клієнта на рахунок в іншому банку України;
- переказ з ПК Клієнта на рахунок іншого клієнта Банку;
- переказ між ПК Клієнта та рахунком Клієнта;
- переказ між поточними рахунками Клієнта;
- переказ з поточного рахунку Клієнта на свою ПК.

2.16.2. У Застосунку передбачена можливість здійснювати наступні види платежів у національній валюті в меню «Перекази», розділ «Платежі», тип платежу «Поповнення мобільного»:

- платіж на поповнення мобільного номера телефону зі своєї ПК.

2.16.3. У Застосунку передбачена можливість здійснювати наступні види обміну валюти в меню «Перекази», розділ «Перекази», тип переказу «Обмін валют»:

- обмін валют між своїми рахунками;
- обмін валют зі свого рахунку на ПК;
- обмін валют зі своєї ПК на свій рахунок;

- обмін валют між своїми ПК.

2.16.4. Для ініціювання переказів/платежів/обміну валют у Застосунку використовується універсальний екран переказів, де Клієнт зазначає дані переказу/платежу/обміну валюти та підтверджує намір здійснити операцію натиснувши на кнопку «Підтвердити», та у разі необхідності вводить OTP пароль з надісланого Банком повідомлення відповідно до вимог Банку.

2.16.5. На універсальному екрані розташовані активні поля для відображення даних переказу/платежу/обміну валюти - **Звідки**, **Скільки**, **Куди,** при натисканні на зазначені поля відбувається перехід на відповідні екрани для вводу/вибору даних Клієнтом, а саме:

• на екран **Звідки**:

❖ для здійснення переказу/платежу/обміну валюти **зі своєї** ПК/ПР Клієнт обирає ПК або Рахунок зі списку, які доступні для відповідного типу переказу;

❖ для здійснення переказу з власної ПК **іншого банку** Клієнт вводить дані (номер, термін дії) ПК вручну (можливе використання функцій Камери для сканування ПК або NFC) чи обирає зі списку збережених та обов'язково вводить CVV2\CVC2.

• на екран **Скільки** (значення суми вводиться через роздільник – крапку, наприклад: 50.00):

❖ для здійснення **переказів/платежів** Клієнт вводить суму переказу/платежу. Валюта відповідає валюті обраної ПК або ПР. Після вводу суми Клієнту відображається сума комісії за переказ, що здійснюється, та загальна сума переказу/платежу, що буде списана з Клієнта;

❖ для здійсненна **обміну валюти** Клієнт вводить суму для обміну валюти, йому відображається розрахункова сума обміну, курс обміну валюти, баланс ПК/ПР списання коштів, виконуються перевірки на відповідність пар валют, лімітів відповідно до вимог передбачених Банком та/або чинним законодавством України.

• на екран **Куди**:

❖ для здійснення переказу/обміну валюти на власну ПК/ПР Клієнт обирає ПК або ПР зі списку ПК/ПР Клієнта, які доступні для відповідного типу переказу/обміну валюти;

❖ для здійснення переказу на ПК іншого клієнта Банку або ПК іншого банку Клієнт вводить номер ПК вручну (можливе використання функцій Камери для сканування ПК або NFC) чи обирає зі списку збережених;

❖ для здійснення переказу на Рахунок в іншому банку Клієнт вводить реквізити одержувача переказу:

- номер рахунку одержувача ;
- найменування одержувача;
- РНОКПП (якщо одержувач – фізична особа) або код ЄДРПОУ (якщо – юридична) в поле «РНОКПП / ЄДРПОУ»;
- призначення платежу (максимум – 420 символів, включаючи номер рахунку та ПІБ власника, які автоматично підставляються при переказі з ПК);

❖ для здійснення платежу поповнення мобільного телефону обирає номер телефону зі списку контактів або вводить номер вручну.

2.16.6. Перелік ПК/ПР, що відображаються на екранах **Звідки, Куди**, можливість вибору та вводу даних ПК/ПР регламентуються згідно з вимогами передбаченими Банком та/або чинним законодавством України для відповідного типу переказу/платежу/обміну валюти.

2.16.7. Банк виконує ініційовані Клієнтом операції за умови, що Клієнт не заблокований у системі Банком.

2.16.8. Банк виконує ініційоване Клієнтом Доручення на договірне списання з власного рахунку/ПК на інший власний рахунок/ПК (переказ) Клієнта за наступних умов:

- попередньо була успішно проведена автентифікація Клієнта у Застосунку;
- ПР/КР/ПК списання є активною, не заблокованою, не закритою;
- рахунок списання має хоча б одну активну ПК (в разі, якщо рахунок списання – КР);
- рахунок/ПК зарахування є активною, не заблокованою, не закритою;
- рахунок зарахування має хоча б одну активну ПК (в разі, якщо рахунок зарахування – КР);
- на рахунку списання/балансі ПК (для КР) на момент ініціювання операції достатньо коштів для здійснення переказу із врахуванням суми комісії (в разі наявності комісії за операцію згідно Тарифів);
- валюта рахунку списання співпадає із валютою рахунку зарахування;
- сума операції не перевищує встановлені ліміти у Застосунку, а у разі виконання переказу з КР – ліміти на здійснення видаткових операцій по КР з використанням ПК.

2.16.9. Банк виконує ініційоване Клієнтом Доручення на договірне списання з рахунку Клієнта на рахунки, відкриті в інших банках України за наступних умов:

- попередньо була успішно проведена автентифікація Клієнта в Застосунку;
- рахунок списання є активним, не заблокованим, не закритим;
- рахунок зарахування є активним, не заблокованим, не закритим;
- рахунок списання має хоча б одну активну ПК (в разі, якщо рахунок списання - КР);
- рахунок зарахування є балансовим рахунком, на який законодавством та/або Банком не заборонено виконувати зарахування коштів;
- на рахунку списання/балансі ПК (для КР) на момент ініціювання операції достатньо коштів для здійснення платежу із врахуванням суми комісії (в разі наявності комісії за операцію згідно Тарифів);
- валюта рахунку списання – національна валюта України;
- сума операції не перевищує встановлені Ліміти у Застосунку, а у разі виконання переказу з КР – ліміти на здійснення видаткових операцій по КР з використанням ПК;
- OTP пароль, що був введений Клієнтом, є вірним.

2.16.10. Банк виконує ініційоване Клієнтом Доручення на переказ з рахунку Клієнта на КР інших клієнтів Банку за наступних умов:
- попередньо була успішно проведена автентифікація Клієнта у Застосунку;
- рахунок списання є активним, не заблокованим, не закритим;
- рахунок списання має хоча б одну активну ПК (в разі, якщо рахунок списання – КР);
- рахунок зарахування є активним, не заблокованим, не закритим;
- рахунок зарахування має хоча б одну активну ПК;
- ПК, відкрита до КР, на яку здійснюється перерахування коштів, емітована Банком та є активною;
- на рахунку списання/ балансі ПК (для КР) на момент ініціювання операції достатньо коштів для здійснення платежу із врахуванням суми комісії (в разі наявності комісії за операцію згідно Тарифів);
- валюта рахунку списання та валюта рахунку зарахування - національна валюта України;
- сума операції не перевищує встановлені Ліміти у Застосунку, а у разі виконання переказу з КР – ліміти на здійснення видаткових операцій по КР;
- OTP пароль, що був введений Клієнтом, є вірним.

2.16.11. Банк виконує ініційоване Клієнтом Доручення на договірне списання з власного рахунку/ПК Клієнта на користь третьої особи (платіж) за наступних умов:
- попередньо була успішно проведена автентифікація Клієнта в Застосунку;
- рахунок/ПК списання є активною, не заблокованою, не закритою;
- рахунок списання має хоча б одну активну ПК (в разі, якщо рахунок списання – КР);
- рахунок зарахування є активним, не заблокованим, не закритим;
- рахунок зарахування є балансовим рахунком, на який законодавством та/або Банком не заборонено виконувати зарахування коштів;
- на рахунку списання/балансі ПК (для КР) на момент ініціювання операції достатньо коштів для здійснення платежу із врахуванням суми комісії (в разі наявності комісії за операцію згідно Тарифів);
- валюта рахунку списання – національна валюта України;
- сума операції не перевищує встановлені ліміти в Застосунку, а у разі виконання переказу з КР – ліміти на здійснення видаткових операцій по КР;
- OTP пароль, що був введений Клієнтом, є вірним.

2.16.12. Банк виконує ініційоване Клієнтом розпорядження на обмін валюти з власного рахунку/ПК на інший власний рахунок/ПК Клієнта за наступних умов:
- попередньо була успішно проведена автентифікація Клієнта в Застосунку;
- рахунок/ПК списання є активним, не заблокованим, не закритим;
- рахунок списання має хоча б одну активну ПК (в разі, якщо рахунок списання – КР);
- рахунок зарахування є активним, не заблокованим, не закритим;
- рахунок зарахування є балансовим рахунком, на який законодавством та/або Банком не заборонено виконувати зарахування коштів;
- на рахунку списання/балансі ПК (для КР) на момент ініціювання операції достатньо коштів для здійснення платежу із врахуванням суми комісії (в разі наявності комісії за операцію згідно Тарифів);
- валюта рахунку списання та валюта рахунку зарахування – відповідають переліку доступних валютних пар;
- сума операції не перевищує встановлені ліміти в Застосунку, а у разі виконання переказу з КР – ліміти на здійснення видаткових операцій по КР;
- OTP пароль, що був введений Клієнтом, є вірним.

2.16.13. Банк на власний розсуд:
- встановлює та змінює Курс Дистанційного обміну валют протягом дня;
- встановлює регламент роботи Дистанційного обміну валют
- визначає доступні операції (купівля/продаж/конвертація) та валютні пари для Дистанційного обміну валют;
- може обмежити право Клієнта купувати валюту за рахунок Кредитного ліміту;
- може встановлювати мінімальну /максимальну суму операції для Дистанційного розпорядження на обмін валют;
- може обмежувати загальну суму купівлі валюти в еквіваленті за офіційним курсом гривні до іноземних валют, установленим Національним банком України на дату здійснення операції Клієнтом протягом дня та/або місяця.

2.16.14. У Застосунку у розділі рахунки/картки Клієнта відображається історія операцій Клієнта, що вплинули на зміну балансу та були ініційовані як Застосунком, так й іншими платіжними інструментами.

2.16.15. Клієнт може повторити виконання операцій, що сформовані у Застосунку та відображені в історії операції з розділу «Історії операцій», натиснувши на необхідну операцію та обравши функціонал «Повторити операцію». У такому випадку дані операції будуть автоматично перенесені на універсальний екран переказів і Клієнт зможе повторити виконання операції.

2.16.16. Для успішно виконаних операцій у Застосунку Клієнт може сформувати квитанцію, для цього йому необхідно вибрати відповідну операцію в «Історії операцій» та вибрати функціонал «Надіслати квитанцію». Після зазначених дій сформується pdf файл з даними операції та електронним підписом Банку. Документ відображається на екрані та стає доступним функціонал поділитися, який дає можливість направити файл на e-mail адресу чи поділитися з контактом за допомогою мессенджерів.

2.16.17. За бажанням звернення до ЦЕНТРУ КЛІЄНТСЬКОЇ ПІДТРИМКИ Клієнт повинен потрясти пристроєм з боку в бік. Після чого автоматично сформується лист із зазначеним e-mail Банку та вкладеним файлом, в якому фіксується інформація щодо роботи Застосунку в цей момент. Клієнту необхідно додати текст звернення та направити листа.

2.16.18. Заява Клієнта про повернення коштів, у разі невдалої сплати в межах сервісу «Платежі», на користь постачальника послуги (організації) приймається до розгляду за умови, якщо статус переказу в Застосунку «Відхилений», кошти були списані та не повернулися на рахунок Клієнта автоматично в поточному та наступному робочому дні, або статус переказу в Застосунку «Проведений», але кошти не дійшли на рахунок постачальника послуги (організації). Заява розглядається Банком протягом 30 днів з моменту її реєстрації в Банку. Після розгляду Заяви Банк повертає кошти на рахунок Клієнта, або надає письмову відповідь Клієнта про неможливість повернення коштів, у разі коректності, успішності проведеної операції та зарахування коштів на користь постачальника послуги (організації).
2.16.19. Ліміти встановлюються Банком для всіх видів переказів на суму однієї операції, та/або на суму операцій за операційний день, календарний місяць відповідно до вимог законодавства та внутрішньої політики Банку та можуть бути змінені.

2.17. Керування послугами

2.17.1. У розділі «Профіль користувача» доступні наступні послуги:
- «Сповіщення» – керування послугою підключення PUSH-сповіщень;
- «Мої картки інших банків» – збереження власних карток інших банків України в список обраних;
- «Податкове резидентство» – оновлення інформації та документів про зміну свого статусу податкового резидентства для цілей Загального стандарту звітності CRS та/або статусу для цілей Угоди FATCA;
- «Інформація про банк» – посилання на Сайт Банку щодо інформації з відомостей про Банк, публічну інформацію, Тарифи, та звернення Клієнтів;
- «Вихід» - здійснення виходу з облікового запису у Застосунку.

2.17.2. Отримання інформації по ПК на детальній формі ПК Клієнта в меню ПК (натискання на зображення карти):
- «Показати номер картки» - відображення повного номеру ПК на зображенні ПК;
- «Показати CVV» – відображається CVV2\CVC2 код до ПК;
- «Скопіювати номер картки» - копіювання номеру ПК.

2.17.3. Керування налаштуваннями по картці на детальній формі ПК Клієнта в меню «Налаштування картки»:
- «Змінити PIN карти» - вводиться новий ПІН-код. Першою операцією для ПК з чипом після установлення ПІН-коду в Застосунку «PIVDENNY ONLINE» має бути операція по ПК з використанням чіпу ПК (перевірка балансу ПК або видача готівки), що проводиться із введенням нового ПІН-коду в банкоматі або платіжному терміналі у відділенні Банку;
- «Переглянути реквізити» – відображаються реквізити карткового рахунку та доступна функція копіювати/надіслати;
- «Платежі за номером телефону» - відображення та керування налаштуванням сервісу за допомогою вмикання/вимикання цього функціоналу;
- «Отримати виписку» - відображається для вибору «Період», «Мова» (українська, англійська) та «Формат документу» (PDF, CSV) та доступна функція надіслати;
- «Отримати Договір» - перегляд Договору на відкриття рахунку у форматі PDF з функцією надіслати (тільки за Договорами які відкриті у мобільному застосунку).
- «Переглянути тарифи» - відображається загальна інформація та основні умови, тарифікація за рахунком, додаткові послуги та надається посиланням на тарифи https://bank.com.ua/tarifi ;
- «Переглянути спеціальні умови» - відображається план, процес та факт виконання спеціальних умов по рахунку.
- «Перевипустити картку» - випуск/перевипуск віртуальної картки до діючого рахунку.
- «Звернутися до служби підтримки» - можливість перейти до месенджерів (Telegram, Viber) або зв'язатись із Банком за телефонами ЦЕНТРУ КЛІЄНТСЬКОЇ ПІДТРИМКИ;
- «Налаштувати ліміти» - встановлення суми лімітів по ПК в розрізі «Готівковий ліміт», «Безготівковий ліміт» та «Ліміт на онлайн-операції» та встановлення лімітів за всіма рахунками в розрізі «Ліміт на миттєві платежі» на добу та «Ліміт суми миттєвого платежу» на операцію;
- «Додати картку до Apple Wallet» - функціонал додавання ПК до гаманця Apple Wallet (на пристроях з ОС iOS);
- «Додати до Google Pay» - функціонал додавання ПК до гаманця Google Pay (на пристроях з ОС Android);
- «Заблокувати картку» - керування блокуванням/розблокуванням ПК (у випадку втрати, крадіжки, компрометації) за допомогою вмикання/вимикання цього функціоналу;
- «Закрити картку» - можливість закриття картки та рахунку.

2.17.4. Для керування послугами в Банку, Клієнт має здійснити наступні дії у Застосунку:
- на головному екрані перейти у відповідне меню;
- обрати потрібний пункт та заповнити необхідні дані;
- у разі необхідності підтвердження дій Клієнта, Банк надсилає повідомлення з OTP паролем в SMS-повідомленні. Клієнт вводить у відповідне вікно Застосунку надісланий код і в разі успішного вводу коду Застосунок вносить відповідні зміни в налаштування послуг Клієнта.

2.17.5. Зазначений перелік послуг у Застосунку, які можуть бути підключені не винятковий та може змінюватись.

2.18. Заходи безпеки при користуванні Застосунком

2.18.1. Для отримання доступу до Застосунку Клієнт зобов'язаний використовувати власний мобільний пристрій.
2.18.2. Політика паролів:
- паролі повинні бути унікальні для кожного Клієнта протягом усього часу роботи системи, містити мінімальна кількість символів – 8, допустимі символи для вводу – латинські літери, цифри та спеціальні символи (! @ $ % ^ & * ( ) _ - +), мінімальна кількість символів у верхньому регістрі – 1, мінімальна кількість символів у нижньому регістрі – 1, мінімальна кількість цифр – 1, мінімальна кількість спеціальних символів – 1.
- термін дії Пароля не може перевищувати 365 днів від дати встановлення постійного Пароля. Зміна Пароля відбувається при вході в Застосунок згідно з вимогами безпеки систем обслуговування клієнтів Банку.

2.18.3. При використанні Застосунку Клієнт повинен:

- якщо вхід у Застосунок виконується з мобільного пристрою третьої особи, то при закінченні роботи з Застосунком виконати Вихід за допомогою відповідного функціоналу в меню «Профіль користувача»;
- стежити за тривалістю сесії (тривалості знаходження в Застосунку без будь-яких дій з боку Клієнта), яка обмежена 15 хвилинами задля безпеки;
- не підключатись до Мобільного застосунку «PIVDENNY ONLINE» через Wi-Fi-точки публічного доступу, які не потребують ідентифікації під час підключення (введення для підключення персонального імені та пароля);
- не встановлювати на телефон/пристрій, який використовується для підключення до Мобільного застосунку «PIVDENNY ONLINE», неліцензійних операційних систем, оскільки це відключає захисні механізми, закладені виробником мобільної платформи;
- для виключення несанкціонованого використання послуг Мобільного застосунку «PIVDENNY ONLINE» не залишати свій телефон/пристрій, який використовується для підключення до Мобільного застосунку «PIVDENNY ONLINE», без нагляду.

2.18.4. Банк за жодних обставин не здійснює:

- розсилку електронних листів із вимогою надіслати Пароль для входу/ PIN-код доступу, Логін та/або інші дані автентифікації та/або не пропонує перейти за вказаною електронною адресою.
- розповсюдження електронною поштою комп'ютерних програм.

2.18.5. При виявленні спроби несанкціонованого доступу до Застосунку необхідно терміново змінити Пароль для входу до Застосунку та звернутися до ЦЕНТРУ КЛІЄНТСЬКОЇ ПІДТРИМКИ для блокування доступу до Застосунку.

3. ПРАВИЛА СТВОРЕННЯ ТА ВИКОРИСТАННЯ ЦИФРОВИХ ТОКЕНІВ

3.8. Загальний опис технології

3.8.1. Банк надає Клієнту (власнику рахунку та Держателю додаткової ПК) послуги дистанційного обслуговування в мобільному застосунку сервісу «Google Pay» компанії Google, в мобільному застосунку сервісу «Apple Pay» компанії Apple, та мобільному застосунку сервісу "Garmin Pay" компанії Garmin. За допомогою мобільного застосунку «Garmin Pay» можна здійснювати розрахунки лише у торгово-сервісній мережі. За допомогою Google Pay та Apple Pay можна здійснювати розрахунки в торгово-сервісній мережі, в мобільних застосунках та на сайтах (для цього мобільний застосунок та/або сайт, на якому виконується платіж, має підтримувати технологію Google Pay/Apple Pay). За допомогою Garmin Pay можна здійснювати розрахунки лише в торгово-сервісній мережі. Пристрій, яким виконується покупка в торгово-сервісній мережі, має підтримувати технологію NFC. Оплата в торгово-сервісній мережі виконується за технологією безконтактних платежів.

3.8.2. Мобільні застосунки «Google Pay»,«Apple Pay» та «Garmin Pay» не зберігають в оперативній або внутрішній пам'яті Мобільного пристрою, або на зовнішніх серверах, дані Платіжної картки. Зберігаються лише дані Токену.

3.8.3. Після встановлення Мобільного застосунку на Мобільному пристрої, Клієнт самостійно ініціює процес Токенізації Платіжної картки – присвоєння картці електронного віртуального цифрового запису – Токену, що замінює номер Платіжної картки. В Мобільному застосунку Клієнту доступні дані про чотири останні цифри платіжного Токену. При виконанні оплати в торгово-сервісній мережі Мобільний пристрій Клієнта обмінюється даними за допомогою функції NFC з Платіжним терміналом за Токеном, тому на Платіжному чеку друкуються дані Токену замість даних ПК Клієнта. При здійсненні оплати в мобільних застосунках або на сайтах, пристрій Клієнта передає мобільному застосунку або сайту дані Токену, тому в електронній квитанції зазначаються дані Токену замість даних ПК.

3.8.4. Номер Токену, присвоєний Платіжній картці Клієнта в рамках даного Мобільного пристрою в процесі Токенізації, може бути застосований лише шляхом застосування конкретного Мобільного пристрою, оскільки Токен прив'язується до конкретного Мобільного пристрою.

Клієнт має можливість здійснити Токенізацію своєї ПК в усіх чотирьох Мобільних застосунках на декількох Мобільних пристроях. Загальна кількість випущених платіжних Токенів до однієї Платіжної картки не може перевищувати 99 штук.

3.8.5. Платіжний Токен являється цифровим аналогом Платіжної картки. До транзакцій, що здійснюються в рамках платіжних Мобільних застосунків «Google Pay»,«Apple Pay» та «Garmin Pay» з використанням електронних цифрових Токенів, застосовуються всі умови Тарифного плану/Тарифів, в рамках яких емітована Платіжна картка Клієнта, та Витратні ліміти, що встановлені за ПК Клієнта, інші ліміти встановлені за ПК, інформація щодо яких розміщена на офіційному сайті Банку https://bank.com.ua.

3.8.6. Строк дії цифрового платіжного Токену становить 5 років з моменту його створення. Статус платіжного Токену копіює статус фізичної ПК. Проведення транзакцій за допомогою платіжного Токену, емітованого до ПК, строк дії якої закінчився/заблокованої ПК/за ПК, прив'язаної до закритого КР, неможливе. У випадку анулювання ПК за будь-якою з причин (закінчення строку дії ПК/закриття рахунку за ініціативою Клієнта/переоформлення картки тощо), Банк автоматично видаляє Токен з пристрою Клієнта. У випадку переоформлення ПК, за якою є активні Токени, за будь-якої з причин (окрім зміни Тарифного плану), Банк автоматично підв'язує випущені платіжні Токени до нової ПК на всіх пристроях, на яких Клієнт токенізував попередню ПК.

3.8.7. Інформація відносно здійснених транзакцій електронним цифровим Токеном в Мобільних застосунках сервісів «Google Pay», «Apple Pay» та «Garmin Pay», відображається безпосередньо на мобільному пристрої/смарт-годиннику/фітнес трекері. В історії платежів відображається 10 останніх платежів, виконаних Токенами. Для того, щоб отримати повну інформацію за всіма транзакціями, Клієнт має отримати Виписку за КР одним із способів запропонованим Банком.

3.8.8. Мобільні застосунки «Google Pay» та «Garmin Pay» не обмежують Клієнта щодо кількості ПК, які можуть бути додані до гаманця на одному пристрої. Мобільний застосунок «Apple Pay» регламентує максимальну кількість цифрових Токенів, що можуть бути створені на одному пристрої, а саме: на пристрої Apple Watch Series 3 або на більш нові моделі, а також iPhone 8, iPhone 8 Plus або на більш нові моделі, можна додати не більше 12 платіжних карток, на більш ранніх моделях можна додати не більше 8 платіжних карток із розрахунку на один пристрій.

3.8.9. Для того, щоб мати можливість зареєструвати картку та користуватися застосунками «Google Pay» та «Apple Pay», Клієнт має встановити один із методів блокування свого пристрою – ПІН/пароль/графічний ключ/відбиток пальця/інші методи). Якщо Клієнт в процесі користування одним із додатків відмовиться від блокування свого пристрою та вимкне відповідні налаштування, створений Токен до ПК автоматично видалиться з пристрою, що унеможливить користування платіжним додатком.
3.8.10. Клієнт має реєструвати кожну ПК в кожному із цифрових гаманців на кожному своєму пристрої окремо за порядком, що описаний нижче для кожного із Мобільних платіжних додатків.
3.8.11. Клієнт має можливість переглянути всі наявні Токени сервісів «Google Pay», «Apple Pay» та «Garmin Pay» ПК у Мобільному застосунку «PIVDENNY ONLINE» Банку на всіх Мобільних пристроях Клієнта на базі операційної системи iOS.
3.8.12. Клієнт має можливість видалити наявний Токен ПК за допомогою Мобільного застосунку «PIVDENNY ONLINE» Банку на базі операційної системи iOS. В такому випадку Токен буде видалено з Мобільних застосунків «Google Pay», «Apple Pay» та «Garmin Pay».

3.9. Користування Мобільним платіжним застосунком сервісу «Google Pay»

3.9.1. Порядок додавання картки до Google Pay на Android безпосередньо в застосунку “Google Pay”:

- завантажити Мобільний застосунок сервісу «Google Pay» на Мобільний пристрій з Play Market.
- ввести дані ПК – номер ПК, строк дії, CVV2/CVC2-код та заповнити дані, що пропонує до заповнення електронний гаманець «Google Pay». Після цього Клієнту присвоюється платіжний Токен в неактивному стані.

Для активації платіжного Токену в системі Банк пропонує Клієнту обрати один із методів автентифікації :
1) отримати одноразовий пароль на Фінансовий номер телефону Клієнта або
2) активувати Токен через ЦЕНТР КЛІЄНТСЬКОЇ ПІДТРИМКИ Банку після проведення процедури Ідентифікації. У випадку, якщо Банк не має можливості надіслати Клієнту Динамічний пароль (за відсутності Фінансового телефону Клієнта), Банк пропонує лише можливість активувати Токен через ЦЕНТР КЛІЄНТСЬКОЇ ПІДТРИМКИ Банку.
Для користування сервісом «Google Pay» Клієнт обов’язково повинен користуватися одним із методом блокування екрану свого Мобільного пристрою (ПІН/ пароль, графічний ключ, відбиток пальця).

3.9.2. Режими здійснення платежів:

3.9.2.2. Розблокований екран Мобільного пристрою – в такому режимі здійснюються платежі на будь-яку суму. У такому випадку Клієнту не потрібно здійснювати вхід безпосередньо до Мобільного застосунку «Google Pay», платіж здійснюється в фоновому режимі;
3.9.2.3. В Мобільному застосунку «Google Pay» - в такому режимі здійснюються платежі на будь-яку суму. У такому випадку Клієнт має розблокувати екран Мобільного пристрою та здійснити вхід до Мобільного застосунку «Google Pay»;
3.9.2.4. Ввімкнений екран мобільного пристрою – в такому режимі здійснюються платежі до порогового значення, встановленого МПС, що авторизується безконтактним способом. У випадку, якщо за такого режиму здійснюється платіж, що перевищує порогове значення, що авторизується безконтактним способом, на екрані Мобільного пристрою з’явиться повідомлення про необхідність розблокувати екран Мобільного пристрою (ввести ПІН/ пароль, графічний ключ, відбиток пальця, Face ID). Клієнт не може самостійно змінювати порогову суму транзакції.
3.9.3. Клієнт може самостійно видалити картку з платіжного гаманця «Google Pay» безпосередньо з Мобільного застосунку. При цьому платіжний Токен також буде видалено.
3.9.4. Клієнт може заблокувати платіжний Токен. Для цього Клієнт має звернутися до ЦЕНТРУ КЛІЄНТСЬКОЇ ПІДТРИМКИ та пройти процедуру Ідентифікації. Клієнт може розблокувати заблокований Токен. Для цього Клієнт має звернутися до ЦЕНТРУ КЛІЄНТСЬКОЇ ПІДТРИМКИ та пройти процедуру Ідентифікації. Клієнт може видалити платіжний Токен. Для цього Клієнт має звернутися до ЦЕНТРУ КЛІЄНТСЬКОЇ ПІДТРИМКИ та пройти процедуру Ідентифікації.

3.10. Порядок додавання картки до Google Pay через мобільний застосунок «PIVDENNY ONLINE»:

Клієнт може додавати бажані активні картки до свого електронного гаманця Google Pay. Щоб додати картку до Google Pay користувач має:

- увійти до Мобільного застосунку;
- обрати активну картку у розділі «Мої картки», відкрити вікно «Налаштування картки» та обрати “Налаштування Google Pay ”.
- натиснути «Додати до Google Pay», після чого мобільний застосунок перепроваджує Клієнта до застосунку Google Pay.

Після проходження необхідних кроків в додатку Google Pay, картка буде додана до гаманця Google Pay для обраного пристрою. Стан кнопки у вікні “Налаштування Google Pay ” зміниться на “Відкрити в Google Pay”.
Після авторизації у застосунку, якщо буде знайдена нова активна карта, яка ще не додана до Google Pay, то буде запропоновано її додати.
У випадку видалення мобільного застосунку, всі додані картки в Google Pay продовжують діяти.
Зверніть увагу, що користувач також має можливість додати картку безпосередньо у застосунку Google Pay.

3.11. Користування Мобільним платіжним застосунком сервісу «Apple Pay»

Порядок додавання картки до Apple Wallet через мобільний застосунок «PIVDENNY ONLINE»:

Клієнт може додавати бажані активні картки до свого електронного гаманця Apple Wallet. Щоб додати картку до Apple Wallet користувач має:
• увійти до Мобільного застосунку;
• обрати активну картку у розділі «Мої картки», відкрити вікно «Налаштування картки» та обрати “Налаштування Apple Pay”.
• натиснути на кнопку «Додати до Apple Wallet», після чого мобільний застосунок перепроваджує Клієнта до застосунку Apple Wallet.
У вікні "Налаштування Apple Pay" користувач може переглянути всі електронні пристрої до яких можливо додати картку (iPhone, iPad, Apple Watch), а також пристрої до яких підключена або призупинена функція Apple Wallet.

Після того, як користувач обирає бажаний пристрій та проходить необхідні кроки в додатку Apple Pay, картка буде додана до гаманця Apple Wallet для обраного пристрою. Стан кнопки у вікні "Налаштування Apple Pay" зміниться на "Додана до Apple Wallet". Якщо у користувача залишаються інші пристрої, які можливо додати до Apple Wallet, кнопка "Додати до Apple Wallet" буде залишатися активною до тих пір, доки Клієнт не додасть картку до Apple Wallet на всіх доступних для нього девайсах. Але якщо у користувача з'явився новий можливий пристрій, кнопка "Додати до Apple Wallet" знову стає активною.
У випадку видалення мобільного застосунку, всі додані картки в Apple Wallet продовжують діяти.
Зверніть увагу що користувач також має можливість додати картку безпосередньо у застосунку Apple Wallet.

Порядок додавання картки до Apple Wallet на iPhone безпосередньо в застосунку "Apple Wallet":

- обрати Wallet та натиснути;
- ввести дані ПК – номер ПК, прізвище та ім'я власника картки, строк дії картки та CVV2 код;
- прийняти правила та умови використання.

Для активації платіжного Токену в системі Банк пропонує Клієнту обрати один із методів автентифікації: 1) отримати одноразовий пароль на Фінансовий телефон Клієнта або 2) активувати Токен через ЦЕНТР КЛІЄНТСЬКОЇ ПІДТРИМКИ після проведення процедури Ідентифікації. У випадку, якщо Банк не має можливості надіслати Клієнту Динамічний пароль (за відсутності Фінансового телефону Клієнта), Банк пропонує лише можливість активувати Токен через ЦЕНТР КЛІЄНТСЬКОЇ ПІДТРИМКИ. У випадку, якщо в момент створення Токена Apple рекомендує Банку здійснити поглиблену ідентифікацію Клієнта, Банк зв'язується з Клієнтом самостійно для того, щоб виявити чи дійсно саме Клієнт додає ПК до Apple Wallet, та у випадку позитивного рішення надсилає Клієнту одноразовий пароль для завершення реєстрації через Систему дистанційного обслуговування «ПІВДЕННИЙ MYBANK» та Клієнт активує Токен.

- натиснути «Далі». Після цього можна розпочати користування Apple Pay.

Порядок додавання картки до Apple Wallet на пристрої iPad:

- обрати «Налаштування» - «Wallet та Apple Pay»;
- натиснути «Додати платіжну картку»;
- ввести дані ПК
- прийняти правила та умови використання.

Для активації платіжного Токену в системі Банк пропонує Клієнту обрати один із методів автентифікації: 1) отримати одноразовий пароль на Фінансовий телефон Клієнта або 2) активувати Токен через ЦЕНТР КЛІЄНТСЬКОЇ ПІДТРИМКИ після проведення процедури Ідентифікації. У випадку, якщо Банк не має можливості надіслати Клієнту Динамічний пароль (за відсутності Фінансового телефону Клієнта), Банк пропонує лише можливість активувати Токен через ЦЕНТР КЛІЄНТСЬКОЇ ПІДТРИМКИ. У випадку, якщо в момент створення Токену Apple рекомендує Банку здійснити поглиблену ідентифікацію Клієнта, Банк зв'язується з Клієнтом самостійно для того, щоб виявити чи дійсно саме Клієнт додає ПК до Apple Wallet, та у випадку позитивного рішення надсилає Клієнту одноразовий пароль для завершення реєстрації через Систему дистанційного обслуговування «ПІВДЕННИЙ MYBANK» та Клієнт активує Токен.

- натиснути «Далі». Після цього можна розпочати користування Apple Pay.

Порядок додавання картки до Apple Wallet на Apple Watch:

- відкрити програму Apple Watch на iPhone та перейти на вкладку «Мій годинник».
- натиснути "Wallet та Apple Pay"
- обрати «Додати кредитну або дебетову картку», ввести дані ПК.
- прийняти правила та умови використання.
- розблокувати Apple Watch шляхом введення паролю.
- натиснути «Далі».

Для активації платіжного Токену в системі Банк пропонує Клієнту обрати один із методів автентифікації: 1) отримати одноразовий пароль на Фінансовий телефон Клієнта або 2) активувати Токен через ЦЕНТР КЛІЄНТСЬКОЇ ПІДТРИМКИ після проведення процедури Ідентифікації. У випадку, якщо Банк не має можливості надіслати Клієнту Динамічний пароль (за відсутності Телефону Клієнта), Банк пропонує лише можливість активувати Токен через ЦЕНТР КЛІЄНТСЬКОЇ ПІДТРИМКИ. У випадку, якщо в момент створення Токену Apple рекомендує Банку здійснити поглиблену ідентифікацію Клієнта, Банк зв'язується з Клієнтом самостійно для того, щоб виявити чи дійсно саме Клієнт додає ПК до Apple Wallet, та у випадку позитивного рішення надсилає Клієнту одноразовий пароль для завершення реєстрації через Систему дистанційного обслуговування «ПІВДЕННИЙ MYBANK» та Клієнт активує платіжний Токен.

- натиснути «Далі». Після цього можна розпочати користування Apple Pay.

Порядок додавання картки на комп'ютері Mac з Touch ID:

- на комп'ютері Mac з Touch ID обрати «Системні налаштування» - «Wallet та Apple Pay»
- натиснути «Додати картку»
- ввести дані ПК
- прийняти правила та умови використання

Для активації платіжного Токену в системі Банк пропонує Клієнту обрати один із методів автентифікації: 1) отримати одноразовий пароль на Фінансовий телефон Клієнта або 2) активувати Токен через ЦЕНТР КЛІЄНТСЬКОЇ ПІДТРИМКИ після проведення процедури Ідентифікації. У випадку, якщо Банк не має можливості надіслати Клієнту Динамічний пароль (за відсутності Фінансового телефону Клієнта), Банк пропонує лише можливість активувати Токен через ЦЕНТР КЛІЄНТСЬКОЇ ПІДТРИМКИ. У випадку, якщо в момент створення Токену Apple рекомендує Банку здійснити поглиблену ідентифікацію Клієнта, Банк зв'язується з Клієнтом самостійно для того, щоб виявити чи дійсно саме Клієнт додає ПК до Apple Wallet, та у випадку позитивного рішення надсилає Клієнту одноразовий пароль для завершення реєстрації через Систему дистанційного обслуговування «ПІВДЕННИЙ MYBANK». Клієнт активує платіжний Токен.

- натиснути «Далі». Після цього можна розпочати користування Apple Pay.

Порядок додавання картки на комп'ютері Mac без Touch ID

Якщо на комп'ютері Mac відсутній Touch ID, можна сплачувати покупки з Apple Pay на сумісному пристрої iPhone або Apple Watch. Для цього на iPhone необхідно перейти в меню «Налаштування» - «Wallet та Apple Pay» та ввімкнути параметр «Можливість сплати на Mac».

3.12. Користування Мобільним платіжним застосунком сервісу «Garmin Pay»

3.12.1. Платіжний застосунок сервісу «Garmin Pay» призначений для власників годинників фірми «Garmin». Для користування даним сервісом необхідний годинник Garmin та смартфон з операційною системою iOS або Android.

3.12.2. Порядок додавання платіжної картки до «Garmin Pay»:

- завантажити мобільний застосунок «Garmin Connect» на смартфон з операційною системою iOS або Android (при цьому не має значення чи підтримує смартфон технологію NFC, оскільки саме годинник Garmin виконує безконтактну оплату, тому важливо, щоб безпосередньо модель годинника підтримувала технологію Garmin Pay).
- відкрити мобільний застосунок «Garmin Connect» на смартфоні, зайти в розділ Garmin Devices та обрати свій годинник.
- натиснути на «Garmin Pay».
- підключити платіжну картку (вказати дані платіжної картки та підтвердити активацію Платіжного токена шляхом введення OTP-пароля з SMS або дзвінком до ЦЕНТРУ КЛІЄНТСЬКОЇ ПІДТРИМКИ.
- встановити пароль, що буде використовуватися для підтвердження здійснення оплати годинником (підтверджується перша транзакція на добу, та/або кожна транзакція, яку було здійснено після зняття годинника з руки).

3.12.3. Порядок здійснення оплати за допомогою «Garmin Pay»:

- зайти в меню на годиннику Garmin
- натиснути іконку з годинником Garmin Pay
- ввести пароль, який було встановлено при додаванні картки (підтверджується перша транзакція на добу, та/або кожна транзакція, яку було здійснено після зняття годинника з руки).
- прикласти годинник до безконтактного терміналу.

3.13. Оплати із застосуванням Click to Pay.

3.13.1. Створення профілю користувача.

Click to Pay передбачає створення профілю користувача Click to Pay, в якому зберігається інформація, надана самим Клієнтом або Банком як уповноваженою Клієнтом особою до МПС Visa/ MasterCard. Банк для створення профілю Click to Pay передає набір інформації до МПС Visa/ Mastercard, яка в сукупності являє собою Платіжну інформацію для Click to Pay.

Клієнт може виконати самостійну реєстрацію своєї Платіжної інформації для виконання оплат Click to Pay. Для цього потрібно скористатися порталом МПС Visa https://secure.checkout.visa.com/ або порталом МПС Mastercard https://src.mastercard.com/profile/enroll?cmp=eemea.uk-ua.eemea.mccom.CreateYourProfile&locale=uk_UA, ввести необхідну Платіжну інформацію для Click to Pay.

Банк створює профіль користувача Click to Pay для Клієнтів, які відповідають критеріям Банку для участі в Click to Pay, без отримання на це додаткової згоди від Клієнта. Критерії Банку для відбору Клієнтів до участі вказуються на Сайті Банку на сторінці https://bank.com.ua/click-to-pay.

Після створення Банком профілю користувача Click to Pay або додавання Банком до профілю нової ПК, Банк інформує про це Клієнта шляхом надсилання йому про це сповіщення.

З метою захисту ПК МПС Visa/ MasterCard генерує цифрові аналоги даних ПК (токени), які будуть використовуватися під час обробки транзакцій та для надання даних ПК точкам електронної комерції та іншим інтернет-сайтам, залежно від придатності ПК для токенізації. Номер ПК та токени зберігаються МПС Visa/ MasterCard та можуть використовуватися для транзакцій.

3.13.2. Оплата з використанням Click to Pay.

Для здійснення оплати з використанням Click to Pay Клієнту необхідно в точці електронної комерції або на інтернет сайті, який підтримує сервіс Click to Pay та на якому відображається значок Click to Pay, обрати спосіб оплати Click to Pay. Перед тим, як Клієнту буде відображено список його карток, доданих до Click to Pay, клієнт має підтвердити свій номер телефону або адресу електронної пошти, які є частиною Платіжної інформації для Click to Pay. У випадку, якщо профіль клієнта в Click to Pay створював Банк, та Клієнт самостійно не вносив інформацію про електронну адресу в свій профіль, підтвердження буде виконуватися по номеру телефону Клієнта. Підтвердження здійснюється шляхом направлення МПС Visa/ MasterCard одноразового OTP коду на номер телефону або електронну адресу клієнта, які є частиною Платіжної інформації Click to Pay. Після того, як Клієнт вперше в браузері, в якому відбувається оплата з Click to Pay, виконає успішне підтвердження OTP коду, браузер запропонує Клієнту зберегти дані. В разі погодження на це з боку Клієнта, дані будуть збережені, подальше проведення оплати з боку Клієнта не потребуватиме верифікації номеру телефону або електронної адреси. Після проходження процедури верифікації номера телефону або електронної адреси, Клієнту відображається перелік його карток, що можуть виконувати оплати з Click to Pay. Клієнт обирає з переліку карток картку для здійснення оплати, і далі платіж відбувається за стандартними протоколами здійснення Інтернет-оплати. Підтвердження платежу відбувається з використанням технології EMV 3DS або Passkey, якщо клієнт надав на це дозвіл на пристрої, на якому він проводить таку оплату.

3.13.3. Припинення участі в Click to Pay.

Клієнт може самостійно відмовитися від участі в Click to Pay. Для цього він може видалити профіль користувача Click to Pay на порталах МПС. Також, клієнт може заблокувати, розблокувати або видалити токен/токени Click to Pay. Для цього Клієнт має звернутися до ЦЕНТРУ КЛІЄНТСЬКОЇ ПІДТРИМКИ. Банк видаляє Платіжну інформацію для Click to Pay із сховища МПС Visa/ MasterCard тоді, коли Клієнт не має жодної Платіжної картки, що підпадає під участь в Click to Pay.