БАНК ПОРТАЛ

АКЦІОНЕРНЕ ТОВАРИСТВО «БАНК «ПОРТАЛ»

ЗАТВЕРДЖЕНО
Рішенням Правління
АТ «БАНК «ПОРТАЛ»,
протокол від 22 липня 2020 року

ПРАВИЛА КОРИСТУВАННЯ ПЛАТІЖНИМИ КАРТКАМИ АКЦІОНЕРНОГО ТОВАРИСТВА «БАНК «ПОРТАЛ»

(діють з 25 серпня 2020 року)

КИЇВ - 2020

1. **Вступ**

1.1. Ці Правила користування платіжними картками АТ «БАНК «ПОРТАЛ» (далі – Правила) визначають основні умови та вимоги безпеки користування платіжними картками (далі – ПК), в тому числі корпоративними платіжними картками, емітованими АТ «БАНК «ПОРТАЛ» (далі – БАНК). Дотримання цих Правил надасть змогу забезпечити КЛІЄНТАМ/уповноваженим особам КЛІЄНТІВ (Держателям ПК) надійне їх зберігання, нерозголошення реквізитів ПК, персонального ідентифікаційного номера (ПІН-коду) та інших даних, а також зменшить можливі ризики під час здійснення операцій з використанням ПК у банкоматах, платіжних терміналах та іншого виду платіжних пристроях, у тому числі через мережу Інтернет.

2. **Визначення і терміни**

2.1. Терміни, які використовуються у цих Правилах, вживаються в значеннях, визначених Договором банківського рахунку, укладеним із КЛІЄНТОМ.

2.2. Інші терміни, які використовуються у цих Правилах, вживаються в значеннях, наведених у нормативно-правових актах Національного банку України, що регулюють правила здійснення операцій з використанням електронних платіжних засобів.

3. **Правила отримання ПК та ПІН-коду, активація ПК**

3.1. Під час отримання ПК Держатель ПК повинен поставити підпис на її зворотному боці в місці, яке призначене для підпису Держателя ПК. Це зменшить ризик незаконного використання ПК.

3.2. Рекомендуємо записати номер своєї ПК та номери телефонів БАНКУ. У випадку втрати ПК, Держателю ПК слід негайно повідомити БАНК.

3.3. Держатель ПК можете самостійно змінити ПІН-код, отриманий в SMS-повідомленні, на будь-яку іншу чотиризначну комбінацію цифр за допомогою банкомату будь-якого банку світу, який надає цю послугу відповідно до вимог Платіжної системи.

3.4. У разі втрати чи забуття ПІН-коду, Держатель ПК може повторно скористуватись послугою замовлення нового електронного ПІН-коду, для чого необхідно звернутись до БАНКУ.

3.5. Активація ПК відбувається:

3.5.1. Уповноваженим працівником БАНКУ за умови проходження Держателем ПК ідентифікації;

3.5.2. працівником Контакт-центру БАНКУ за умови здійснення телефонного дзвінка та проходження Держателем ПК ідентифікації.

4. **Загальні правила використання ПК, ПІН-коду та коду CVC2**

4.1. ПК використовується в будь-якому торгівельному закладі та пункті видачі готівки, де розташований логотип відповідної Платіжної системи.

4.2. Держатель ПК не повинен розголошувати ПІН-код та код CVC2 стороннім особам (членам родини, знайомим, працівникам БАНКУ, особам, які намагаються допомогти під час використання ПК).

4.3. ПІН-код необхідно запам'ятати або записати та зберігати його окремо від ПК у місці, недоступному для сторонніх осіб.

4.4. Забороняється передавати ПК для використання стороннім особам. Забороняється розголошувати та повідомляти персональні дані або інформацію про ПК на вимогу будь-яких сторонніх осіб, у тому числі і працівників БАНКУ, крім надзвичайних випадків (звернення до БАНКУ для здійснення операцій з використанням ПК).

4.5. ПК необхідно зберігати у місці, недоступному для сторонніх осіб та віддаленому від джерел температурного та електромагнітного випромінювання.

4.6. З метою підвищення безпеки зберігання коштів на Рахунку БАНКОМ за замовчуванням встановлюються Первинні авторизаційні ліміти та Авторизаційні

ліміти на здійснення операцій з використанням ПК, які розміщуються на сайті БАНКУ.

4.7. КЛІЄНТ, в межах Авторизаційних лімітів, має право встановити Індивідуальні ліміти на отримання готівки та здійснення покупок за сумою та за кількістю операцій, крім граничних лімітів з отримання готівки, які має право встановлювати Національний банк України відповідно до законодавства, шляхом надання письмової заяви до БАНКУ або шляхом звернення КЛІЄНТА (зателефонувавши) до Контакт-центру. Ініціювати зміну Індивідуальних лімітів за Додатковими ПК має право особа, котрій відкрито у БАНКУ рахунок, за яким випущено ПК.

4.8. З метою запобігання незаконним операціям з використанням ПК, БАНКОМ при відкритті рахунку автоматично здійснюється підключення послуги SMS-інформування про проведені операції з використанням ПК.

4.9. Якщо ПК втрачено чи викрадено (у т.ч. і за кордоном), Держатель ПК повинен заблокувати ПК шляхом телефонного звернення до Контакт-центру БАНКУ.

4.10. Для здійснення перевипуску ПК, КЛІЄНТОВІ необхідно звернутись до БАНКУ з відповідною заявою про перевипуск ПК.

4.11. Якщо ПК пошкоджена або з іншої причини стала непридатною для використання, необхідно звернутись до БАНКУ із відповідною заявою про перевипуск ПК.

4.12. Якщо ПІН-код став відомий сторонній особі, Держателю ПК необхідно здійснити операцію «Зміна ПІН-коду» в будь-якому банкоматі світу, який надає цю послугу відповідно до вимог Платіжної системи.

4.13. У разі забуття ПІН-коду до ПК, Держателю ПК необхідно звернутись до БАНКУ за перевипуском ПІН-коду.

4.14. У системі моніторингу БАНКУ здійснюється постійна перевірка на ознаки можливих шахрайських дій з використанням ПК БАНКУ, у т. ч. і по транзакціях, що відбуваються за кордоном. В ході моніторингу транзакцій, БАНК може заблокувати операцію по ПК, по якій виникла підозра на шахрайські дії з боку третіх осіб. Якщо ПК заблоковано, Держатель ПК може звернутися до Контакт-центру БАНКУ для отримання інформації щодо причини блокування.

4.15. При здійсненні операцій через банкомати, платіжні термінали/пристрої тощо може вимагатися введення ПІН-коду. У випадку 3 (трьох) спроб набору неправильного ПІН-коду, ПК вилучається та її дія призупиняється. Для розблокування ПК, КЛІЄНТОВІ необхідно звернутися до Контакт-центру БАНКУ.

5. Правила користування банкоматом

5.1. Перед використанням банкомата необхідно оглянути його щодо наявності додаткових приладів, які не відповідають його конструкції та розташовані в місці набору ПІН-коду або в місці, призначеному для прийому ПК (наприклад, наявність нерівно встановленої клавіатури для набору ПІН-коду).

5.2. Якщо клавіатура або місце для прийому ПК банкомата обладнані додатковими пристроями, що не відповідають його конструкції, Держатель ПК не повинен використовувати даний банкомат для здійснення операцій з використанням ПК і має повідомити про це банк за номером телефону, який зазначено на банкоматі.

5.3. ПІН-код необхідно набирати таким чином, щоб особи, які перебувають поруч, не змогли його побачити. Під час набору ПІН-коду необхідно прикривати клавіатуру рукою. Якщо банкомат працює некоректно (наприклад, довгий час перебуває в режимі очікування, перезавантажується), необхідно відмовитись від послуг такого банкомата та скасувати поточну операцію, натиснувши на клавіатурі кнопку «Відміна» («Отмена» чи «CANCEL») і дочекатись повернення ПК.

5.4. Після отримання готівки в банкоматі необхідно її перерахувати та переконатись у тому, що ПК була повернена банкоматом, дочекатись видачі чеку в разі його запиту і тільки після цього відходити від банкомату. Роздруковані банкоматом чеки потрібно зберігати для звірки зазначених у них сум з випискою про рух коштів за рахунком.

5.5. Під час проведення операції через банкомат може виникнути ситуація, коли банкомат не повертає ПК. Причинами цього може бути:

5.5.1. збій в роботі банкомата (ПК не видана протягом 1,5 - 2 хвилин);

5.5.2. закінчення ліміту часу, відведеного для того, щоб забрати ПК (ПК не забрана КЛІЄТОМ протягом 30-35 секунд);

5.5.3. інше.

У даному випадку КЛІЄНТОВІ необхідно звернутись до БАНКУ і тимчасово заблокувати ПК.

5.6. Для отримання вилученої або нової ПК необхідно звернутися до БАНКУ.

6. Правила здійснення безготівкових розрахунків з використанням ПК

6.1. Держатель ПК не повинен використовувати ПК в торговельній мережі для оплати товарів або послуг, якщо торговець/продавець/касир викликав у нього недовіру.

6.2. Розрахунки з використанням ПК повинні здійснюватися лише у присутності Держателя ПК. Це забезпечить зниження ризику розголошення персональних даних Держателя ПК, зазначених на ПК.

6.3. Під час використання ПК для оплати товарів або послуг продавець/касир може вимагати від Держателя ПК надати паспорт, підписати квитанцію або ввести ПІН-код. Перед набором ПІН-коду необхідно переконатися, що треті особи, які перебувають у безпосередній близькості, не зможуть його побачити. Перед тим, як підписати квитанцію, необхідно в обов'язковому порядку перевірити суму, що зазначена на ній.

6.4. Потрібно зберігати чеки, що підтверджують факт здійснення операції з використанням ПК, до моменту відображення відповідних операцій у щомісячній виписці.

6.5. При здійсненні операції за кордоном, банк, що обслуговує банкомат або платіжний пристрій, у тому числі в мережі Інтернет, може запропонувати КЛІЄНТОВІ виконати операцію з використанням Динамічної конвертації.

6.6. Динамічна конвертація передбачена правилами Платіжних систем, а сама конвертація здійснюється не за курсом Платіжної системи або емітента картки, а виключно за курсом банку, що обслуговує банкомат або платіжний пристрій (банку-еквайра), у тому числі в мережі Інтернет.

6.7. При виборі КЛІЄНТОМ Динамічної конвертації, операція здійснюється не у валюті країни перебування, а у валюті, встановленій за замовчуванням для банка-емітента ПК. Проведення такої операції може призвести до списання з Рахунку КЛІЄНТА більшої суми, ніж вказана на екрані банкомату або платіжного пристрою при проведенні операції. Це відбувається через конвертацію суми, що виставлена Платіжною системою БАНКУ до погашення за проведеною операцією у валюту Рахунку КЛІЄНТА на день розрахунку з ПС за курсом конвертації валют БАНКУ на день проведення відповідного розрахунку.

6.8. Для всіх ПК БАНКУ валютою «за замовчуванням» є гривня.

6.9. Пропозиція про використання послуги «Динамічна конвертація» може вказуватися на екрані банкомату або платіжного пристрою в момент виконання операції або може буди ідентифікована як пропозиція провести операцію за кордоном у валюті «за замовчуванням» для ПК БАНКУ.

6.10. За КЛІЄНТОМ завжди залишається право відмовитись від послуги Динамічної конвертації і провести операцію у валюті країни, де здійснюється операція.

7. Правила здійснення операцій через мережу Інтернет

7.1. Використання ПІН-коду під час замовлення товарів або послуг через мережу Інтернет, а також за телефоном/факсом, не передбачене правилами платіжних систем і свідчить про шахрайський характер операції. В жодному випадку Держатель ПК не повинен здійснювати такі операції.

7.2. Для придбання товарів та послуг в мережі Інтернет необхідно використовувати відомі Держателеві ПК інтернет-сайти і перевірені інтернет-магазини.

7.3. Не потрібно робити повторних спроб оплатити рахунок безліч разів. Це може призвести до блокування БАНКОМ можливості провести платіж, так як може спрацювати система безпеки БАНКУ від підбору параметрів ПК.

7.4. Якщо оплата товару (послуги) здійснюється через чужий комп'ютер, після завершення всіх розрахунків, необхідно переконатися, що реквізити ПК та інша конфіденційна інформація не збереглась на даному комп'ютері. Для цього необхідно знову відкрити сторінку продавця, на якій здійснювалась оплата товару, та переконатись, що відповідні поля бланку-замовлення перебувають у незаповненому стані.

7.5. На комп'ютер, з якого регулярно здійснюються операції з використанням ПК, необхідно встановити антивірусне програмне забезпечення і вчасно здійснювати його оновлення, а також оновлення інших програмних продуктів (операційної системи, прикладних програм). Це зменшить ризик «зараження» комп'ютера вірусними програмами, які здійснюють викрадення персональних даних.

8. Термін дії ПК та перевипуск ПК

8.1. Термін дії ПК вказано на її лицьовій стороні ПК дійсна до останнього дня місяця, вказаного на ній, включно.

8.2. Для перевипуску ПК КЛІЄНТОВІ необхідно звернутись до БАНКУ протягом останнього місяця терміну дії ПК.

Голова Правління **Р. М. Піддубний**