

## **Правила користування платіжними картками**

Терміни та поняття, які використовуються у цих Правилах, вживаються у значеннях, які визначені Договором про комплексне банківське обслуговування фізичних осіб.

### **1. Платіжна картка.**

1.1. Держатель ПК одержує ПК у відділенні Банку вигляді пластикової картки та /або у вигляді Віртуальної картки (її реквізити) в смс-повідомленні, відправленому на Фінансовий номер телефону та у Мобільному застосунку.

1.2. При випуску Карток Банк встановлює базові Ліміти на проведення кожного типу операцій з використанням Картки. Клієнт може змінити ці Ліміти звернувшись до відділення Банку, Контакт-центру чи в Мобільному застосунку.

З метою зменшення ризиків проведення незаконних операцій з використанням ПК доцільно змінювати добовий ліміт на суму та кількість операцій із застосуванням ПК тільки на час проведення операцій а також відслідковувати повідомлення Банку з інформуванням про здійснені операції.

### **2. Заходи безпеки при користуванні Карткою, втрата Картки або незаконне використання.**

2.1.3 метою запобігання несанкціонованому використанню Картки та попередження пов'язаних з цим збитків Клієнт (Користувач) повинен дотримуватися наступних правил та рекомендацій:

2.1.1. При отриманні Картки поставити з її зворотного боку свій підпис (у разі відсутності підпису на Картці, якщо це передбачено правилами Платіжної системи, касир має право відмовитися від здійснення операції з використанням Картки);

2.1.2. Зберігати в таємниці, не розголошувати нікому, в тому числі членам власної родини, паролі до Мобільного застосунку, індивідуальну облікову інформацію та/або іншу інформацію, що дає змогу ініціювати Платіжні операції, реквізити Картки, такі як, номер Картки, ПІН – код, CVV2/CVC2, строк дії Картки, одноразові 3D Secure чи OTP-паролі, та не передавати Картку в користування іншим особам;

2.1.3. Не зберігати ПІН-код разом з Карткою, не записувати його на Картці, періодично змінювати ПІН-код. У разі зміни ПІН-коду, обирати надійний ПІН-код. Не рекомендується у якості ПІН-коду використовувати дати народження чи інші дані, які можна пов'язати з Клієнтом;

2.1.4. При спілкуванні з представниками Банку або для здійснення переказу ніколи не повідомляються такі дані: PIN-код картки; термін її дії; три цифри на звороті картки CVV2/CVC2; паролі, що надходять із SMS; 3DS Secure коди; пароль до Інтернет-банкінгу; ІМЕІ та PUK коди до телефону та сім-карти мобільного оператора.

2.1.5. Перед отриманням коштів через Платіжні пристрої, переконатись у тому, що на пристрої для видачі готівки, на пристрої, який приймає картку, та на клавіатурі відсутні

будь – які зайві пристрої;

2.1.6. Не використовувати Платіжний пристрій для отримання коштів та/або інших операцій з ПК у разі виявлення або підозри наявності підозрілих пристроїв, встановлених на картоприймач, відсік для прийому/видачі коштів та /або інші частини Платіжного пристрою;

2.1.7. Не надавати Картку (реквізити Картки) у користування іншим особам;

2.1.8. Ініціювати операції, що не суперечать законодавству, а також не використовувати Картку з метою, що не відповідає чинному законодавству України;

2.1.9. Перед отриманням коштів через Платіжний пристрій проводити візуальний огляд Платіжного пристрою на наявність скімінгових та/або підозрілих сторонніх пристроїв переконатись у тому, що на пристрої для видачі готівки, на пристрої, який приймає Картку, та на клавіатурі відсутні будь-які зайві пристрої;

2.1.10. При проведенні касиром платіжної операції з використанням ПК тримати її в полі свого зору для контролю дій касира щодо проведення повторних операцій чи інших несанкціонованих дій;

2.1.11. Перевірити правильність суми та інших умов проведення операції, зазначених на чеку платіжного терміналу та/або сліпі. Підписанням чека та/або сліпа Клієнт ідентифікує себе, погоджується з умовами проведення операції та підтверджує правильність її суми, яка буде списана з Поточного рахунку з використанням ПК;

2.1.12. Зберігати документи, що підтверджують проведені операції, до моменту їх відображення у Виписці;

2.1.13. При телефонному зверненні в Банк надавати ідентифікаційну/верифікаційну інформацію про себе;

2.1.14. Забезпечити технічну можливість отримання смс-повідомлень/Push – повідомлень в Мобільному застосунку/ повідомлень у месенджер з метою контролю руху коштів за своїм Поточним рахунком з використанням ПК та негайного повідомлення в Банк про операції, які не виконувались;

2.1.15. Встановлювати на Мобільний пристрій додатки лише з надійних джерел;

2.1.16. Не встановлювати на телефоні / пристрої, що використовується для підключення телефону Клієнта або використовуваному для підключення до Мобільного застосунку неліцензійні операційні системи, так як це відключає захисні механізми, закладені виробником мобільної платформи;

2.1.17. Не підключатися до Мобільного застосунку через Wi-Fi точки публічного доступу, які не вимагають ідентифікації при підключенні (введення для підключення персональних імені та пароля);

2.1.18. Не передавати свій Мобільний пристрій у користування іншим особам, в тому числі неповнолітнім дітям, іншим членам сім'ї;

2.1.19. Щоб виключити неналежне використання послуг у Мобільному застосунку, не залишати свій телефон/пристрій, з використанням якого здійснюється отримання Клієнтом послуг, без нагляду;

2.1.20. Відслідковувати операції, що здійснюються за Поточним рахунком з використанням Картки, у разі виявлення факту незаконного використання Картки Клієнт повинен негайно повідомити про це Банк;

2.1.21. Негайно повідомити Банк шляхом (звернення до Контакт- центру або відділення Банку) про втрату або крадіжку Мобільного пристрою, на який встановлений

Мобільний застосунок та/або Картки, підозру на несанкціоноване використання Картки або її реквізитів, а також про те, що ПІН – код став відомий іншій особі;

2.1.22. У разі втрати або крадіжки індивідуальної облікової інформації, Карток або у випадку їх компрометації, а також у випадку подання до Банку заяви щодо оскарження шахрайських операцій з використанням Картки, негайно після того, як Клієнту стало відомо про факт втрати такої інформації та/або платіжного інструменту (Картки) та/або Фінансового номеру телефону, та/або компрометації індивідуальної облікової інформації (або іншої інформації, що дає змогу ініціювати Платіжні операції), повідомити Банк шляхом звернення до Контакт-центру або до відділення для блокування Картки (внести Картку в Стоп-список);

2.1.23. Не пізніше **3 (трьох) Робочих днів** після усного повідомлення звернутися до Банку з клопотанням про оформлення нових Карток у зв'язку з їх втратою/ крадіжкою/ компрометацією, шляхом безпосереднього подання до Банку письмової заяви;

2.1.24. Не піддавати ПК дії електромагнітного випромінювання (не тримати її поруч з мобільними телефонами, магнітами, побутовою, відео – /аудіотехнікою тощо), впливу високих температур та агресивних середовищ;

2.1.25. Повернути Картку/ Картки в Банк не пізніше ніж в день закриття Поточного рахунку з використанням ПК або протягом **3 (трьох) Робочих днів** з моменту отримання повідомлення про розірвання Договору з ініціативи Банку.

### **3. Персональний ідентифікаційний номер**

3.1. ПІН є одним із засобів захисту від несанкціонованого використання ПК.

3.2. З метою захисту грошових коштів на Поточному рахунку з використанням ПК Банк забороняє Клієнту (Користувачу) розголошувати ПІН іншим особам ПК. Розголошення ПІН іншій особі розглядається Банком як грубе порушення цих Правил і може призвести до розірвання Договору за ініціативою Банку.

### **4. Застосування ПК**

4.1. Використання ПК здійснюється для:

4.1.1. оплати товарів та послуг у безготівковій формі в усіх уповноважених установах і підприємствах (в т.ч. в мережі Internet), які приймають до оплати ПК Вашого типу;

4.1.2. отримання/внесення готівкових коштів у банківських установах або за допомогою Платіжних пристроїв (банкоматів, програмно-технічних комплексів самообслуговування тощо);

4.1.3. здійснення платежів та переказів коштів з ПК;

4.1.4. отримання інформації про залишок на Поточному рахунку з використанням ПК;

4.1.5. зміни ПІН-коду в банкоматах або за зверненням до Контакт-центру Банку;

4.1.6. будь-які інші операції з використанням ПК, які не заборонені законодавством України та дозволяються до проведення Платіжною системою, до якої належить Ваша ПК;

4.2. Для успішної платіжної операції за кордоном доступний залишок на Поточному рахунку з використанням ПК повинен бути на 10% більше суми транзакції разом з комісією, якщо така передбачена Тарифами Банку. Ця вимога стосується лише блокування суми під час здійснення операції. Списання з Поточного рахунку з

використанням ПК відбудеться згідно Тарифів Банку.

При проведенні транзакцій на зарубіжних ресурсах, в тому числі в торгово-сервісній мережі, мережі Інтернет, а також, при отриманні готівкових коштів, Банк, з метою запобігання виникнення недозволеного (несанкціонованого) овердрафту за рахунком з використанням ПК може блокувати для використання Клієнтом суму, що складає 5% від суми початкової транзакції. Розблокування заблокованої суми відбудеться одразу після отримання Банком підтвердження на списання з рахунку грошових коштів за початковою транзакцією, при цьому, сума, яка стане доступною клієнту буде залежати від суми грошових коштів, списаних за початковою транзакцією. Таким чином, якщо сума списання за основною транзакцією буде перевищувати суму початкової авторизації, різниця буде списана з рахунку Клієнта за рахунок блокування.

4.3. Для проведення розрахунків за придбані товари або надані послуги необхідно пред'явити працівнику ТСП ПК. За правилами прийому до оплати ПК у деяких торгових та сервісних організаціях у Клієнта (Користувача) можуть попросити пред'явити паспорт або інший документ, що засвідчує особу. Тому при користуванні ПК Банк рекомендує мати при собі відповідний документ, що посвідчує особу.

4.4. Працівник уповноваженого ТСП має право звірити підпис Клієнта (Користувача), поставлений в його присутності на чеку із підписом на зворотній стороні ПК. Якщо працівник ТСП не впевнений в ідентичності підпису, він має право запропонувати Клієнту (Користувачу) повторно розписатися на чеку (в окремих випадках декілька разів, до тих пір, поки не переконається в ідентичності підпису).

4.5. У разі помилки при заповненні чека Клієнт (Користувач) повинен вимагати його знищення у особистій присутності.

4.6. Для розрахунків в мережі Internet Банк рекомендує користуватися окремою ПК: не зберігати на ній кошти, а поповнюйте безпосередньо перед здійсненням транзакції на суму покупки. Для цього можна скористатися сервісами переказів коштів між платіжними картками. Використання ПК для розрахунків в мережі Internet має підвищений ризик. Одноразово вказавши ваш номер на будь якому з веб-сайтів Ви ризикуєте розкрити доступ до Ваших коштів шахраям, які можуть використати вашу ПК через деякий термін. Пам'ятайте, що 90% усіх спірних транзакцій було зроблено у мережі Internet. Банк зробить усе можливе для повернення коштів Клієнта, але відповідальність за ці операції не Клієнт.

## **5. Отримання готівки.**

### **5.1. За допомогою банкомату**

5.1.1. Умовою для отримання готівки за Карткою через банкомат є правильне введення ПІН – коду та наявність коштів на Рахунку. У випадку неправильного введення ПІН – коду, банкомат запропонує ввести його ще раз. В разі триразового невірнього введення ПІН – коду, Картку буде заблоковано/вилучено банкоматом.

5.1.2. Операція з отримання готівки в банкоматі вважається правильно здійсненою і не може бути скасована за умови виконання всіх необхідних для її здійснення дій (введення Картки в карткоприймач Банкомата, набір ПІН – коду, вибір та підтвердження здійсненої операції).

5.1.3. Для отримання готівки за допомогою банкомату переконайтесь, що банкомат працює (екран дисплея висвічує надпис привітання).

Перед використанням банкомат Ви повинні 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).

Якщо клавіатура або місце для прийому ПК банкомата обладнані додатковими пристроями, що не відповідають його конструкції, Ви не повинні використовувати даний банкомат для здійснення операцій з використанням ПК.

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

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 на Поточному рахунку з використанням ПК.

У разі видачі банкоматом невірної суми Клієнт (Користувач) має право надати Банку заяву на оскарження операції з описом обставин її проведення та надати ксерокопію чека (за його наявності). Банки повністю контролюють і фіксують всі операції в своїх платіжних пристроях, тому при черговій інкасації буде проведена перевірка фактичного залишку коштів у ньому. Якщо операція, за якою суму було видано неправильно здійснена в платіжному пристрої, що належить Банку, залишок на Рахунку Клієнта буде приведено у відповідність з фактичними операціями (Рахунок буде збільшено на не отриману суму або зменшено на отриманий надлишок) після завершення процедури перевірки обставин спірної операції. За операціями, здійсненими в платіжних пристроях інших банків, кошти будуть повернуті на Рахунок після здійснення Банком процедур, строки яких встановлюються правилами відповідної Платіжної системи.

При вилученні Картки через технічний збій в роботі банкомату, невірне введення ПІН – коду або у випадку, коли Клієнт (Користувач) не забрав (–ла) Картку з картоприймача, Клієнту (Користувачу) необхідно звернутися до Контакт-центру Банку для блокування Картки та повідомити про всі обставини, пов'язані з вилученням Картки, а також отримати інструкції щодо подальших дій.

Для отримання вилученої ПК Клієнт (Користувач) повинен звернутися до банку, якому належить банкомат, що вилучив ПК.

Проте Банк наполегливо рекомендує замовити перевипуск ПК в будь-якому найближчому відділенні Банку, враховуючи високий ризик компрометації вилученої ПК. Банк не несе відповідальності за подальше користування ПК, яка була вилучена банкоматом іншого банку, та повністю перекладає відповідальність за цей ризик на Клієнта.

### **Примітка.**

➤ **Завжди майте під рукою номер телефону Банку для екстреного зв'язку з Банком.**  
➤ **Завжди зберігайте виписки за підсумками операції, які видає банкомат. Це дозволить вести облік знятих грошей і контролювати списання грошей з Вашого Поточного рахунку з використанням ПК.**

**Увага! Отримання суми готівки в банкоматах може бути обмежене, згідно правил міжнародних платіжних систем, законодавства України, внутрішніх розпоряджень банків.**

### **5.2. В установах банків в межах/поза межами України**

Видача готівки здійснюється у касовому залі уповноваженого банку, відміченого позначками (логотипами) відповідних міжнародних платіжних систем.

**Для отримання готівки за допомогою POS-терміналу** надайте касиру банку Вашу ПК та паспорт, або інший документ, що посвідчує особу та відповідно до Законодавства України може бути використаним на території України для укладення правочинів) для підтвердження Вашої особи. Також касир може вимагати введення ПІН – коду на спеціальній клавіатурі імпринтера. У такому випадку, Ви повинні ввести ПІН – код самостійно, не повідомляючи його касиру.

Касир зобов'язаний:

- перевірити реквізити ПК;
- проавторизувати Вашу ПК (надіслати запит до банку, в якому відкрито Ваш Поточний рахунок з використанням ПК);
- надати відповідний документ із зазначенням суми, що запитується, Вам на підпис.

Після отримання чека, зробіть на ньому підпис (попередньо перевіривши відповідність суми, що вказана на чеку, із сумою що запитується). У разі неповної відповідності підпису на чеку із підписом на Вашій ПК, касир має право запросити підпис ще раз. Отримавши готівку, ПК та оригінал чеку, уважно перерахуйте гроші не відходячи від каси.

**Для отримання готівки за допомогою імпринтера** (пристрій, призначений для перенесення рельєфних реквізитів ПК на сліп для формування первинних документів) необхідно надати касиру ПК.

Касир зобов'язаний заповнити сліп та запросити поставити на ньому Ваш підпис. Отримавши від Вас сліп та поставивши на ньому свій підпис – отримати від авторизаційного центру підтвердження про можливість проведення авторизації.

У разі отримання повідомлення з авторизаційного центру:

- > «відмовити в авторизації» - касир зобов'язаний відмовити в отриманні готівки та знищити у Вашій присутності підписаний Вами сліп;
  - > «вилучити картку» – касир зобов'язаний вилучити Вашу ПК, у Вашій присутності розрізати її, знищити підписаний Вами сліп та видати розписку, що ПК була вилучена.
- Увага! Попередження - при отриманні готівкових коштів в касі (POS-терміналі) іншого банку, може бути утримана додаткова комісія.**

### **Платежі за допомогою ПК за товари та послуги:**

#### **5.3.Оплата товарів і послуг у торгово – сервісній мережі**

5.3.1.При використанні Картки для оплати товарів/послуг Клієнт (Користувач) зобов'язаний підтвердити оплату вірним введенням ПІН-коду та/або скористатися сервісами які забезпечують такі розрахунки після введення відповідного паролю до мобільного пристрою (інше), та/або підписати розрахунковий документ, заздалегідь пересвідчившись, що правильно зазначені номер картки, сума, валюта і дата операції. Підписуючи даний документ, Клієнт (Користувач) визнає правильність вказаної суми, що надає Банку право на списання коштів з Рахунку. Клієнт (Користувач) повинен отримати одну копію оформленої квитанції (чеку).

5.3.2.ТСП, що приймають Картки для оплати товарів чи послуг, мають право, якщо таке право передбачено правилами Платіжної системи, вимагати від Клієнта (Користувача Картки) пред'явлення паспорта чи іншого документу, що підтверджує особу, а також повідомлення інформації, що дозволяє ідентифікувати його як законного Користувача Картки, а також введення ПІН – коду для проведення авторизації.

5.3.3.При проведенні операції видачі готівки через Платіжний пристрій або здійснення розрахунків в ТСП касир може отримати відповідь щодо заборони проведення операції:

- у разі отримання відповіді «відмовити» касир повинен повернути Користувачу Картку;
- в разі отримання відповіді «вилучити Картку» касир повинен вилучити Картку, видати Користувачу ПК розписку про факт її вилучення. При цьому Користувач ПК повинен пересвідчитися, що Картку надрізано касиром для того, щоб уникнути її використання іншими особами.

5.3.4.Якщо оплачений Карткою товар або послугу повернено або не одержано в повному обсязі, Користувач ПК самостійно повинен звернутись до ТСП, у якій було придбано товар або надана послуга. Працівник ТСП виписує кредитовий чек/сліп (Credit Voucher) на суму поверненого товару/послуги. Банк зараховує на Рахунок відповідну суму згідно із кредитовим чеком/сліпом в строки, встановлені правилами Платіжних систем.

5.3.5.У разі, якщо відміна операції здійснюється на наступний робочий день після її проведеної або пізніше та сума операції вже списана з Рахунку, Банк зараховує кошти за операцією на Рахунок. У разі, якщо відміна операції здійснюється в день її проведення, відповідна сума не списується з Рахунку, але є недоступною для використання протягом строку, встановленого правилами та вимогами Платіжної

системи.

5.3.6. Повернення коштів на Рахунок можливе виключно в безготівковій формі у строки передбачені правилами відповідної Платіжної системи.

5.3.7. При неотриманні коштів по кредитовому чеку/сліпу протягом 45 днів з дня оформлення кредитового чеку/сліпа, Користувач ПК повинен повідомити про це Банк для врегулювання питання з ТСП та надати цей кредитовий чек/сліп.

Використання Картки з метою, що не відповідає законодавству, у тому числі з метою оплати товарів або послуг, обіг яких заборонено законодавством, забороняється. У випадку виявлення Банком факту використання Картки для здійснення протиправних дій Банк залишає за собою право надання інформації у правоохоронні органи згідно з встановленим законодавством порядком.

**Увага!**

**Необхідно зберігати копії усіх чеків та сліпів, що одержані Користувачем ПК, та є підтвердженням платежів ПК за товари та послуги. Зберігання цих документів допоможе запобігти невідповідностей у списанні коштів з Поточного рахунку з використанням ПК.**

**Якщо при здійсненні оплати за товари або послуги розрахунок здійснювався готівковими коштами, після невдалих спроб розрахуватися ПК, потрібно зберігати чеки (сліпи) за такими операціями. Зберігання цих документів допоможе запобігти невідповідностей у списанні коштів з Поточного рахунку з використанням ПК.**

## **5.4. Оплата товарів і послуг через інтернет**

5.4.1. У разі здійснення оплати за товари, роботи або послуги в мережі Internet необхідно уважно ставитися до вибору сайту, що здійснює приймання Платіжних карток до сплати. Віддавати перевагу відомим Вам торговцям та намагатися уникати розміщення інформації про Платіжну картку на невідомих сайтах. Використовувати захищені сайти.

5.4.2. Для здійснення операції в мережі Internet (оплати за товари/послуги, підписка на будь-які платні розсилки тощо), на сайті продавця необхідно внести у відповідні позиції реквізити ПК: номер ПК, дату закінчення терміну дії ПК (ММ/РР – місяць та рік) та код SVC2/CVV2 (три цифри вказані поруч з панеллю для підпису).

5.4.3. У разі, якщо здійснюються операції ручного введення (МО/ТО транзакції – Mail Order/Telephone Order) (операції Manual), Вами по телефону, факсом чи під час безпосереднього спілкування повідомляються торговцю номер ПК та дата її закінчення (код SVC2/CVV2 в жодному разі не повідомляється). Після цього оператором/касіром здійснюється операція Manual в мережі Internet, при чому, для такої операції перевірка коду SVC2/CVV2 повинна бути відключена. Для відключення перевірки коду CVV2 слід зателефонувати в Контактний центр Банку, де, після Вашої ідентифікації, замовити відключення перевірки на певний, потрібний Вам, період часу. Операції Manual найчастіше використовуються під час бронювання готелів чи оренді автомобілів. Якщо Ви зарезервували номер в готелі за допомогою ПК та бажаєте відмінити таке резервування, необхідно зробити анулювання резервування. В протилежному випадку з ПК буде списано суму, еквівалентну сумі проживання в даному готелі протягом однієї



добу. Необхідно надати запит працівнику готелю, що повідомляє Вам код анулювання, письмове підтвердження анулювання резервування номеру готелю, що має містити прізвище та ім'я Держателя ПК, номер ПК, за допомогою якої було зроблене резервування, строк її дії, код анулювання та інші дані, що стосуються відміни резервування. Письмове підтвердження анулювання дозволить вирішити спірні ситуації, у разі їх виникнення, на Вашу користь.

**Увага!** При здійсненні за кордоном оплати за товари або послуги деякі торговці можуть запропонувати здійснити операцію у валюті країни емітента ПК (в гривні) – сервіс Dynamic Currency Conversion (DCC). Торговець має право виконати операцію на зазначених умовах тільки після попередньо отриманої згоди клієнта, при цьому самим торговцем визначається курс обміну. Деякі сайти, під час здійснення операції безготівкових розрахунків в мережі Internet, так само можуть пропонувати здійснити розрахунки у валюті країни банку - емітента. Не слід користуватись такими сервісами, адже з кореспондентського рахунку Банку все одно буде списано долари США (євро) і операція буде визначатись як така, що пройшла у валюті списання. У цьому разі, якщо Поточний рахунок з використанням ПК було відкрито в гривні, то здійснюватиметься списання суми операції за комерційним курсом Банку та стягнення комісії Банку за обмін валюти.

**Увага!** При здійсненні оплати за товари або послуги торговець може стягувати додаткову комісію. Торговець повинен попередньо повідомити Клієнта про наявність та розмір такої комісії.

## **6. Особливості використання Картки у країнах підвищеного ризику**

6.1. Банк, з метою зниження ризику використання міжнародної платіжної Картки у незаконних (шахрайських) цілях, рекомендує Користувачам ПК бути особливо уважними при користуванні Карткою в країнах, що визнані міжнародними платіжними системами високоризиковими.

6.2. При виїзді за кордон (чи намірі розрахуватись в мережі Internet на сайті зазначених країн) Держатель ПК зобов'язаний повідомити про це Банк звернувшись до Контакт-центру Банку для встановлення відповідних лімітів розрахунків.

6.3. У разі, якщо Користувач ПК має намір використати Картку для розрахунку в одній з країн, що визнані міжнародними платіжними системами високоризиковими, Банк рекомендує здійснювати покупки за допомогою Картки тільки у великих магазинах відомих брендів, а отримувати готівку – у відділеннях всесвітньо відомих банків, аеропортах або готелях міжнародних мереж.

6.4. Відновлення заборони здійснюється за телефонним повідомленням власника Поточного рахунку з використанням ПК. Список країн підвищеного ризику для здійснення операцій з використанням платіжних карток розміщується на Офіційному сайті Банку.

## **7. Вилучення ПК**

7.1. ПК може бути вилучена працівниками уповноваженого підприємства, в якому Ви

маєте намір розрахуватися за допомогою ПК. Працівник повинен пояснити причину вилучення ПК. Як правило, такою причиною є відповідне розпорядження Банку.

7.2. Якщо банкомат, через який Ви мали намір отримати готівкові кошти, не повернув ПК, необхідно терміново надати інформацію Банку за номером: 0 800 3 111 33; (044) 585 14 87.

## **8. Дії при втраті або крадіжці ПК та/або індивідуальної облікової інформації.**

8.1. У разі втрати або крадіжки ПК, підозри на несанкціоноване її використання Клієнту (Користувачу ПК) необхідно негайно заблокувати ПК за допомогою Мобільного застосунку або звернутися до Контакт-центру за номером телефону: 0 800 3 111 33; (044) 585 14 87 або надати заяву до відділення Банку. У разі звернення до Контакт-центру Користувач ПК повинен надати інформацію для його ідентифікації. При телефонному зверненні Користувача ПК до Контакт-центру ПК блокується шляхом її внесення до Стоп-списку. Блокування Картки здійснюється в момент виконання відповідної операції у Мобільному застосунку або телефонного звернення Користувача ПК та його ідентифікації. Після блокування ПК, здійснення операцій з нею, які потребують авторизації, стане неможливим: на авторизаційний запит Банк надасть відмову або вказівку «вилучити Картку». (Банк стягує плату за послуги, пов'язані з блокуванням Картки та її перевипуском, згідно з Тарифами. Банк стягує плату шляхом списання коштів з Рахунку (якщо оплату не було здійснено готівкою через касу Банку). Усі витрати, пов'язані з послугою із блокування ПК та її перевипуском за ініціативою Клієнта, несе Клієнт).

8.2. Користувач ПК повинен впевнитись, що усне повідомлення було зафіксовано. Після надання повідомлення про факт та обставини втрати або крадіжки ПК/індивідуальної облікової інформації, Користувач ПК повинен записати прізвище працівника Банку, який отримав повідомлення, залишити свої координати та номер телефону, за яким з ним можна зв'язатися протягом 48 годин.

8.3. **ВАЖЛИВО:** До моменту повідомлення Банку про факт втрати ПК та/або індивідуальної облікової інформації ризик збитків від виконання неналежних платіжних операцій та відповідальність за них покладаються на Клієнта. Клієнт несе відповідальність в повному обсязі за всі операції, що супроводжуються Авторизацією, при наявності доведених випадків, що дії чи бездіяльність Клієнта призвели до втрати Платіжної картки, втрати/розголошення даних до емітованого платіжного інструменту (ПК) та іншої індивідуальної облікової інформації Клієнта (ідентифікаційних даних та/або номера мобільного телефону, на який здійснюється відправлення одноразових цифрових паролів та додаткових засобів автентифікації), якщо ПК не поставлена в Стоп-список.

З моменту повідомлення Клієнтом про факт втрати ПК та/або індивідуальної облікової інформації ризик збитків від виконання неакцептованих/неналежних Платіжних операцій та відповідальність покладаються на Банк. Моментом, з якого настає відповідальність Банку, є момент, з якого Клієнт повідомив Банк про факт втрати платіжного інструменту (ПК) та/або індивідуальної облікової інформації та Банк поставив Картку в Стоп-список.

Клієнт несе повну відповідальність за неналежне використання або отримання

грошових коштів з Платіжної картки (в тому числі Віртуальної картки) третіми особами у разі, якщо буде доведено, що дії чи бездіяльність Клієнта (Користувача) призвели до втрати платіжного інструменту (Картки, Мобільного пристрою) або індивідуальної облікової інформації, розголошення ПНУ/індивідуальної облікової інформації або іншої інформації, яка дає змогу ініціювати платіжну операцію з використанням платіжного інструменту.

8.4. При знаходженні вкраденої чи загубленої ПК, заблокованої відповідно до цих Правил, Клієнт (Користувач ПК) зобов'язаний терміново повідомити про це Банк зателефонувавши до служби підтримки Контактного центру Банку 0 800 3 111 33; (044) 585 14 87 або за заявою звернувшись до відділення Банку. Відновлення користування нею можливе тільки після її розблокування. Розблокування Картки проводиться у Мобільному застосунку або на підставі звернення Користувача ПК до Банку, крім випадків, коли таке розблокування є технічно неможливим (в іншому випадку відновлення користування ПК можливе тільки в разі її заміни). ПК буде вилучено з Стоп – списку в строк до одного робочого дня після отримання Банком зазначеної заяви. Відновлення користування Карткою, заблокованою відповідно до цих Правил, можливе в разі випуску нової карти. Випуск нової картки здійснюється на підставі на підставі звернення Користувача ПК до Банку після оплати цієї послуги відповідно до Тарифів та здачі знайденої Картки в Банк.