Правила користування міжнародними платіжними картками АТ "Ідея Банк" для уникнення випадків підвищеного ризику збитків для користувача електронного платіжного засобу

---

1. Користування БПК та ПІН-кодом

Банківська платіжна картка (надалі - БПК), видана Держателю, є власністю Банку. Для безпеки та для мінімізації ризиків здійснення несанкціонованих операцій держатель платіжної картки повинен дотримуватися наступних правил, щодо використання:

1.1 ПІН-коду. Зберігати його в таємниці, щоб ні за яких умов він не став відомий третім особам, при введені ПІН-коду завжди прикривайте ПІН-клавіатуру пристрою в якому необхідно ввести ПІН-код (наприклад рокую);

1.1.1 не зберігати ПІН-код на будь-яких цифрових носіях, не записувати ПІН-код на Платіжній Картці, в мобільному телефоні або в інших місцях, до яких існує можливість доступу сторонніх осіб;

1.1.2. знищувати повідомлення, які містять ПІН-код одразу після ознайомлення з їх змістом;

1.1.3. Застосовувати всі розумні заходи для попередження втрати/крадіжки/вилучення БПК або її несанкціонованого використання;

1.1.4. не передавати БПК з повідомленням ПІН-коду, а також коди доступу або іншу інформацію, яка дає змогу ініціювати операції у користування третім особам (наприклад: строк дії БПК; CVV2/CVC2 – кодів; кодів з SMS-повідомлення), надійно зберігати БПК.

1.2 Банківської платіжної картки. Держатель несе відповідальність за збереження конфіденційності інформації щодо одноразових паролів, паролів, ПІН-кодів, інших засобів доступу до портативного пристрою, Мобільного платіжного додатку, БПК, Токену;

1.2.1. обмежити та недопускати третіх осіб до портативного пристрою, Мобільного платіжного додатку, БПК, Токену шляхом встановлення паролів (цифрових, графічних тощо), біометричних ідентифікаторів тощо;

1.2.2. забезпечити безпеку портативного пристрою та Мобільного платіжного додатку, встановити та своєчасно оновлювати антивірусні програми.

1.3 Користування карткою в банкоматах. Використовувати БПК у надійних банкоматах (у відділеннях, у торгових центрах або в банкоматах АТ «Ідея Банк» або банках партнерів), при цьому:

1.3.1. під час введення ПІН-коду прикривати клавіатуру долонею;

1.3.2. використовувати послугу зняття без картки.

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

1.4 Оплати в супермаркетах:

1.4.1. використовувати безконтактну оплату PayPass, Google Pay, Apple Pay;

1.4.2. не передавати картку в руки касирові під час розрахунків;

1.4.3. після здійснення платежу за товари та послуги за допомогою Картки, уважно перевіряти отриманий від касира-продавця чек, в якому вказана сума що сплачується. Сума вказана на чеку повинна відповідати сумі, що висвічується на електронному табло терміналу.

Увага! Наполегливо радимо зберігати копії усіх чеків, що одержані Вами, та є підтвердженням платежів Карткою за товари та послуги. Зберігання цих документів допоможе запобігти невідповідностей у списанні коштів з Вашого Рахунку.

Для проведення операції платіжна картка проходить авторизацію. Якщо валюта операції відрізняється від валюти карткового рахунку, платіжна система самостійно перераховує суму авторизації в валюту карткового рахунку за курсом, встановленим платіжною системою на день здійснення авторизації, та блокує дану суму на платіжному ліміті картки. Списання суми з карткового рахунку по операції, валюта якої відрізняється від валюти карткового рахунку, відбувається по комерційному курсу Банку, встановленому на день здійснення такого списання.

2. Втрата, нестандартні ситуації та незаконне використання БПК.

2.1. Якщо Ваша Картка загублена чи викрадена або Ви втратили пристрій з програмним забезпеченням, що дає змогу здійснити операцію за допомогою Токена, то необхідно негайно (в момент виявлення) повідомити Банк шляхом звернення за телефоном **0800 505 203** та дотримуватись отриманих інструкцій співробітника Банку, або повідомити через СДО ІО (функція «Тимчасове блокування») або через Месенджери.

2.2. Звернутися у Банк із заявою про виготовлення нової БПК при її втраті чи пошкодженні (протягом 3-х днів з моменту втрати/пошкодження), а також при умові, якщо ПІН-код став відомий третім особам.

3. Банк не несе відповідальності за:

3.1. несанкціоновані Клієнтом операції за допомогою БПК/реквізитів БПК з використанням ПІН-коду та/або CVV2/CVC2 – кодів, здійснені до отримання Банком повідомлення Клієнта про втрату/несанкціоноване використання БПК та/або ПІН-коду;

3.2. несанкціоновані Клієнтом операції за допомогою БПК здійснені без авторизації у разі відмови Клієнта від застосування встановленого Банком Щоденного ліміту;

3.3. збитки завдані Клієнту внаслідок не отримання ним sms-повідомлення Банку про здійснення операції, якщо воно належно відправлене оператором мобільного зв'язку на Фінансовий номер або інший номер мобільного телефону Клієнта;

3.4. якість товарів (послуг), придбаних Клієнтом за допомогою БПК.

Увага! Якщо операція виконана з використанням технології 3-D Secure або її аналогу тобто при здійсненні операцій з використанням БПК та/або її реквізитів, при якій для завершення операції з використанням БПК та/або її реквізитів, держатель зобов'язаний ввести оригінальний числовий пароль, що надходить на номер мобільного телефону у вигляді SMS-повідомлення. У випадку введення числового паролю всі операції, підтверджені таким чином, вважаються проведеними безпосередньо держателем та не можуть бути оскаржені як несанкціоновані Клієнтом.

4. Термін дії БПК та видача нової картки.

Термін дії БПК проставлено на її лицьовій стороні. Картка дійсна до останнього дня вказаного на ній року та місяця включно. Якщо не порушено умови Договору, дія старої БПК припиняється у встановленому порядку. Після цього Держатель звертається на відділення Банку, де відкритий його рахунок, за новою карткою. Власник рахунку відповідає за те, щоб всі БПК даного рахунку після припинення терміну їх дії були повернені в Банк. Якщо додаткова чи корпоративна БПК занесена в "стоп-лист", то її Держатель може надати в Банк заяву про видачу нової БПК лише за письмовою згодою Власника рахунку.

5. Безпека карткових операцій:

5.1. Заходи безпеки під час користування смартфоном

5.1.1. Сучасні телефони та планшети дозволяють обмежити доступ до пристрою за допомогою пароля, ПІН-коду, графічного ключа тощо.

5.1.2. Захистіть свої персональні ПК, смартфони і планшети від вірусів

5.2. Безпека під час купівель в Інтернеті

5.2.1 Якщо ви продаєте товар на інтернет-майданчику, для отримання переказу на картку за продаж товару необхідно зазначити лише номер картки;

5.2.2 Не залишайте номер свого фінансового телефону в Інтернеті;

5.2.3 Використовуйте лише популярні та перевірені сайти;

5.2.4 Не переходьте і не оплачуйте послуги за посиланнями, отриманих від незнайомих людей або у SMS-повідомленнях або за скороченими лінками;

5.2.5 Будьте обережні при виборі товарів/послуг із занадто привабливими пропозиціями

5.2.6 Застосовуйте технологію 3-D Secure або її аналог при здійсненні операцій з використанням БПК та/ або її реквізитів.

Важливо! Секретний код 3D Secure або його аналог – ні працівники Банку, ні Інтернет-сайти не можуть бачити. Захист 3D Secure – це одноразовий динамічний секретний код, який генерується системою для кожної операції з використанням платіжної картки MasterCard на Інтернет-сайтах, які підтримують технологію 3D Secure. Технологія 3D-Secure надається безкоштовно за умови, якщо для картки активована послуга SMS-інформування про операції з платіжною карткою. Послугу SMS-інформування можна підключити через Інтернет-Банкінг або звернутися до Контакт-Центр Банку.

6. Методи протидії шахраям

6.1 Ніколи не надавайте інформацію про свої картки третім особам, навіть якщо вони звертаються до вас нібито від імені банку. Ідея Банк має всю необхідну інформацію для забезпечення Вашого обслуговування. Банк не телефонує й не надсилає повідомлень, щоб попросити клієнтів зазначити номер банківської картки, строк її дії, ПІН-код або CVV2-код картки, пароль до системи інтернет- банкінгу, а також паролі, що надходять в SMS-повідомленнях.
6.2. Будьте пильні, якщо вам приходять SMS-повідомлення невідомого авторства, щодо будь-якого використання картки її блокування із зазначенням номерів для зворотного зв'язку. В таких випадках рекомендуємо:
6.2.1 Уважно перевіряти інформацію - від кого саме надійшло SMS-повідомлення. Банк відправляє SMS-повідомлення, в адресі якого вказане доменне ім'я (напр. IdeaBank)
6.2.2 За жодних обставин не телефонуйте на вказані в SMS-повідомленні телефонні номери.
6.2.3 Звертайтеся до Банку тільки за номером, вказаним на звороті картки або ж на офіційному сайті.
6.2.4 Повідомте Банк про отримане SMS-повідомлення. Після консультації з представником Банку, номер, з якого надійшло SMS-повідомлення, потрібно внести у чорний список телефону, а саме повідомлення - видалити.

7. Ліміт на картку та високо-ризикові країни
7.1. Піклуючись про безпеку своїх клієнтів та з метою мінімізації ризиків проведення шахрайських операцій за платіжними картками, АТ «Ідея Банк» впровадив нову систему добових лімітів на готівкові та безготівкові операції. Дані ліміти встановлені за замовчуванням та можуть бути змінені за бажанням клієнта у будь-який момент.
7.2. З метою підвищення безпеки використання платіжних карток та для мінімізації ризиків здійснення несанкціонованих операцій, для всіх платіжних карток АТ «Ідея Банк» діють обмеження на готівкові та безготівкові операції на території країн, які відповідно до статистичних та нормативних даних відносяться до країн з високим ризиком здійснення шахрайських операцій. Отже, якщо ви плануєте закордону подорож, будь-ласка, проінформуйте представника банку та тимчасово зніміть обмеження з платіжної картки для використання у країні з підвищеними ризиком. Для цього достатньо просто зателефонувати до Контакт-Центру Ідея Банку за телефоном 0 800 50 20 30. Номер телефону для зв'язку у роумінгу +38 0342 55 87 62 (тарифи згідно оператора зв'язку). З деталями можна ознайомитися за посиланням https://ideabank.ua/uk/security