**РЕКОМЕНДАЦІЇ ДЕРЖАТЕЛЯМ ПЛАТІЖНИХ**

**КАРТОК АТ «БАНК 3/4» ЩОДО ПРОВЕДЕННЯ**

**БЕЗПЕЧНИХ РОЗРАХУНКІВ**

Шановний Клієнте, АТ «БАНК 3/4» радить Вам дотримуватись цих рекомендацій, сподіваємось, це допоможе Держателям платіжних карток, що емітовані АТ «БАНК 3/4», знизити ризики втрат під час здійснення операцій із використанням платіжної картки в банкоматах, під час безготівкової оплати товарів/послуг (у тому числі через мережу Інтернет), сприятиме їх надійному зберіганню та безпеці розрахунків.

Рекомендації діють в частині, що не суперечить Правилам користування платіжною карткою, емітованою АТ «БАНК 3/4» і поширюються на всі платіжні картки, які емітовані АТ «БАНК 3/4» (далі -Банк).

**І. Загальні рекомендації для Держателів платіжних карток АТ «БАНК 3/4»**

1. Запам’ятайте ПІН-код та зберігайте його окремо від платіжної картки (далі – Картки) та гаманця в недоступному для сторонніх осіб місці.

2. Не зберігайте ПІН- код на смартфоні або ноутбуці/планшеті.

Не зберігайте окремо від Картки в одному місці СVC2/CVV2 разом з номером картки та/або строком її дії.

3. Не слід передавати Картку іншим особам (у тому числі родичам). Персоніфіковану платіжну картку (що містить прізвище та ім’я фізичної особи) має право використовувати виключно та фізична особа, чиє ім’я нанесено на Картку.

4. Банк ніколи не здійснює запити та/або телефонні дзвінки своїм клієнтам – Держателям платіжних карток щодо перевірки реквізитів виданої Картки або уточнення персональних даних (серія, номер паспорта, ідентифікаційний номер, персональний пароль, номер мобільного телефону тощо). Не розголошуйте та не повідомляйте реквізити Картки (номер, ПІН, СVC2/CVV2, термін дії), власні персональні дані або будь-яку іншу інформацію, що стосується Картки на вимогу сторонніх осіб (у тому числі й працівників банку). У разі виникнення такої ситуації одразу телефонуйте до Банку за телефонами Клієнтської підтримки 0800503434, +380443649828, і повідомте про цей факт (Клієнтської підтримки Банку, зазначено на зворотному боці Картки).

5. Ніколи не передавайте реквізити Картки через відкриті канали інформаційного обміну: електронну пошту, смс, соціальні мережі, месенджери, чати, тощо. Якщо повідомляєте третій особі номер Картки для одержання переказу коштів, ніколи не повідомляйте строк дії картки та/або СVC2/CVV2 (останні два реквізити не потрібні для ініціювання переказу).

6. Доцільно мати при собі номер платіжної картки та контактні телефони Банку на інших носіях інформації (у записнику, мобільному телефоні, персональному комп’ютері тощо), але в жодному випадку не разом із записом про ПІН – код/ СVC2/CVV2.

7. Доцільно встановити добовий витратний ліміт на суму та кількість операцій із застосуванням Картки та підключити послугу GSM-banking. Це послуга оповіщення про проведені операції (наприклад, у вигляді коротких текстових повідомлень на мобільний телефон (смс), засобами електронної пошти або в інший спосіб) з метою запобігання незаконним діям/сумнівним операціям з використанням платіжної картки (та/або її реквізитів) та зняття коштів з Вашого рахунку.

8. Не слід відповідати на електронні листи, телефонні дзвінки та смс, у яких ніби від імені Банку пропонується надати персональні дані (такі листи в більшості випадків розсилаються шахраями та зловмисниками). Банк дійсно може звертатись до Клієнта з метою актуалізації даних чи уточнення деталей операцій. Однак, при цьому Банку не потрібно уточнення реквізитів карток/рахунків. В разі ведення листування з Банком переконливо радимо перевірити на веб-сайті Банку <https://bank34.ua/> адресу Банку (відділення), а також адресу електронної пошти. У випадку виникнення сумнівів, будь ласка, самостійно зателефонуйте до Клієнтської підтримки Банку та уточніть інформацію.

9. Не слід відкривати посилання (сторінки/сайти/портали тощо) у мережі Інтернет, зазначені в таких “листах-розсилках” (у тому числі включаючи офіційну сторінку Банку), оскільки це можуть бути *підробні* (сторінки-двійники), через які можуть здійснюватися незаконні дії/сумнівні операції з використанням даних вашої Картки. Зазвичай, такі адреси мають дуже схоже написання, що відрізняється на 1 знак (наприклад, пробіл, кома, літера).

10. Для забезпечення безпеки та в цілях інформаційної взаємодії з Банком рекомендуємо використовувати виключно ті реквізити засобів зв’язку (мобільних, стаціонарних телефонів, сторінок у мережі Інтернет (сайтів/порталів), пошти/електронної пошти тощо), які зазначені в документах, отриманих безпосередньо в Банку, які надавалися при видачі Картки.

16. У разі втрати Картки Держатель повинен негайно повідомити про це Банк. Банк не несе відповідальності за переказ коштів за допомогою такої платіжної картки, ініційований до отримання відповідного повідомлення.

17. Запам’ятайте, що розголошення ПІН -коду, персональних даних, реквізитів Картки чи її втрата суттєво підвищує ризик здійснення незаконних дій з боку третіх осіб та сприяє зникненню коштів з Вашого рахунку.

18. Взаємовідносини Банка та Клієнта за операціями з використанням платіжних карток установлюються укладеним Договором про надання банківських послуг (далі – Договір), Правилами банківського обслуговування фізичних осіб в АТ «БАНК 3/4», які оприлюднені на сайті Банку [www.bank34.ua](http://www.bank34.ua).

19. Держатель Картки повинен самостійно та постійно контролювати стан банківського рахунку та відстежувати рух коштів за всіма операціями, які він здійснював. Держатель може бути як Клієнтом, так і особою, на ім’я якої Клієнт замовив випуск Картки. З Держателем, якщо він не є власником рахунку, Банк не укладає Договір, але проводить ідентифікацію та верифікацію Держателя. За дії Держателя відповідає Клієнт.

20. Рекомендуємо щомісяця отримувати від Банку (у будь-який зручний спосіб: поштою, засобами електронної пошти, факсом тощо) виписку за Вашим рахунком.

21. Перед тим, як виїхати закордон, обов’язково перевірте термін дії Картки та переконайтеся, що у Вас достатньо коштів на рахунку. Також доцільно переконатись, що всі Ваші обов’язкові платежі та платежі за обслуговування рахунку, зроблені вчасно. У разі потреби – поповніть рахунок.

22. У країнах із високим ризиком шахрайства Банком можуть бути встановлені додаткові обмеження на проведення операцій із використанням Карток. Тож, якщо Ви плануєте подорож до однієї з таких країн – зверніться до Банку для уточнення деталей. Ви можете зняти обмеження на використання Вашої Картки або встановити інші добові ліміти.

**ІІ. Рекомендації Держателям платіжних карток Банку щодо застосування**

**їх у банкоматах**

23. Перед проведенням операції з отримання готівкових коштів у банкоматі, огляньте його щодо наявності додаткових приладів, які не відповідають та/або суттєво відрізняються від його конструкції і розташовані в місці набору ПІН -коду, у отворі, призначеному для приймання карток чи видачі коштів (наприклад, наявність нерівно встановленої клавіатури для набору ПІН- коду). У разі виявлення зазначеного не використовуйте такий банкомат.

24. Якщо клавіатура або місце для приймання Карток чи видачі коштів банкомата обладнані додатковими пристроями, що не відповідають його конструкції, не використовуйте його для здійснення операцій з використанням платіжної картки і повідомте про це Банк телефоном, який зазначено на банкоматі.

25. Рекомендуємо здійснювати операції з використанням платіжних карток через банкомати, які встановлені в безпечних місцях (наприклад, у банках, установах та організаціях, великих торговельних комплексах, готелях, аеропортах тощо).

26. Не використовуйте пристрої, які потребують уведення ПІН -коду для доступу в приміщення, де розташовано банкомат.

27. Не застосовуйте фізичну силу, щоб вставити Картку в отвір, призначений для приймання платіжних карток. Якщо Картка легко не вставляється, то не слід використовувати такий банкомат.

28. Набирайте ПІН -код таким чином, щоб особи, які перебувають поруч, не змогли його побачити. Під час набору ПІН-коду прикривайте клавіатуру рукою.

29. Не здійснюйте операцій через банкомат/термінал самообслуговування, якщо Вам не зрозуміле його меню або інформація на екрані. Також не слід використовувати банкомати та термінали, якщо на них містяться невідомі пристрої та ті, що розташовані в підозрілих неосвітлених місцях.

30. Якщо банкомат працює некоректно (наприклад, довгий час перебуває в режимі очікування, мимоволі перезавантажується тощо) відмовтеся від послуг такого банкомата, відмініть поточну операцію, натиснувши на клавіатурі кнопку “Відміна” (“Отмена” чи “CANCEL”) і дочекайтеся повернення платіжної картки.

31. Після отримання готівки в банкоматі необхідно її перерахувати. Переконайтесь у тому, що Картка була повернена банкоматом. Отримайте чек (у разі його запиту). Лише після зазначених вище дій слід відходити від банкомата.

32. Роздруковані банкоматом чеки потрібно зберігати для можливості контролю та звірки зазначених у них сум з випискою про рух коштів за рахунком.

33. Не слід проводити ніяких дій за підказками/порадами сторонніх осіб. Не радимо також приймати від них жодної допомоги під час здійснення операцій через банкомат із використанням Картки.

34. Якщо під час проведення операції із використанням банкомата Картка не повертається, то необхідно зателефонувати до банку за телефоном (який зазначено на банкоматі) та описати ситуацію, що склалася, а також звернутися з цього приводу до АТ «БАНК 3/4» за телефонами Клієнтської підтримки 0800503434, +380443649828, для встановлення причин порушень та/або можливих технічних збоїв у роботі банкомата чи самої Картки. Рекомендуємо заздалегідь записати номер Клієнтської підтримки в телефонний довідник.

**ІІІ. Рекомендації Держателям платіжних карток Банку**

**щодо проведення безготівкових розрахунків**

35. Будьте уважні, не поспішайте. Відповідайте за власні дії. Не вимагайте від торговця/продавця/касира/оператора здійснити операцію за картками сторонніх осіб (зокрема за карткою чоловіка/дружини/батьків/дітей тощо). У такий спосіб Вас можуть запідозрити, як шахрая (зловмисника) та направити до Вас працівників служби безпеки торговельно-сервісного підприємства або поінформувати Банк чи правоохоронні органи.

36. Забороняється під час здійснення безготівкових розрахунків передавати Картку або чек для підпису третім особам чи неповнолітнім дітям.

37. Не використовуйте Картку в торговельній мережі для оплати товарів або послуг, якщо торговець/продавець/касир/оператор/адміністратор (у ресторані, магазині, на АЗС тощо) викликав у Вас недовіру.

38. Розрахунки з використанням Картки мають виконуватися тільки у Вашій присутності. Це забезпечить зниження ризику неправомірного отримання персональних даних, зазначених на Картці.

39. Під час використання Картки для оплати товарів або послуг продавець/касир/оператор може вимагати від Держателя Картки надати паспорт, підписати квитанцію або ввести ПІН.

40. Перед набором ПІН- коду слід переконатися, що треті особи, які перебувають у безпосередній близькості, не зможуть його побачити.

41. Перед тим, як підписати квитанцію, в обов’язковому порядку перевірте суму, зазначену на ній.

42. Якщо під час здійснення оплати товарів або послуг з використанням Картки не вдалося успішно здійснити операцію, то необхідно зберігати один примірник виданої терміналом квитанції для перевірки відсутності зазначеної операції у виписці про рух коштів за рахунком.

43. У випадках вилучення Картки третіми особами відповідно до законодавства України, вимагайте у особи, що вилучає Картку, розписку про її вилучення.

44. Пам’ятайте, що платіжна картка – як готівка. Не залишайте її без нагляду.

**ІV. Рекомендації Держателям платіжних карток Банку**

**щодо здійснення операцій у мережі Інтернет**

45. Не слід використовувати ПІН-код під час замовлення товарів або послуг через мережу Інтернет, а також телефоном/факсом.

46. Не повідомляйте інформацію про Картку або картковий рахунок через мережу Інтернет (відправка даних через e-mail, Telegram, Viber, тощо), наприклад ПІН - код, паролі доступу до рахунків, термін дії Картки, СVC2/CVV2, кредитні ліміти, персональні дані тощо.

47. З метою запобігання незаконним діям або сумнівним операціям з використанням даних Картки рекомендуємо для оплати товарів (послуг) через мережу Інтернет використовувати окрему Картку, наприклад Картку Virtual з обмеженим лімітом на розрахунки.

48. Необхідно використовувати сторінки в мережі Інтернет (сайти/портали) тільки відомих і перевірених Інтернет-магазинів які використовують захищене з’єднання (адреса сайту Інтернет-магазину, повинна починатися з «https://» та\або мати піктограму «замочок» перед адресою).

49. Рекомендуємо не сканувати QR-коди на сторінках/сайтах, що викликають підозру.

50. Не слід використовувати систему Інтернет-банкінг через публічні мережі Wi-Fi (насамперед у кафе, барах, ресторанах, парках, готелях тощо).

51. Рекомендуємо оплату проводити через сервіси Google Pay, Apple Pay або сертифіковані платіжні сервіси (наприклад, LiqPay, Portmone, iPay, Fondy, EasyPay, тощо). Обов’язково переконайтесь у правильності зазначення адреси сторінок у мережі Інтернет (сайтів/порталів), до яких підключаєтесь і через які збираєтеся здійснювати оплату товарів (послуг), оскільки схожі адреси можуть використовуватися для здійснення незаконних дій або сумнівних операцій з використанням персональних даних платіжної картки. Сайт на якому плануєте виконувати оплату має використовувати захищене з’єднання (адреса сайту, повинна починатися з «https://» та\або мати піктограму «замочок» перед адресою).

52. Рекомендуємо здійснювати оплату товарів (послуг), придбаних через мережу Інтернет, тільки зі свого комп’ютера з метою збереження конфіденційності персональних даних та/або інформації про рахунок. При цьому не рекомендуємо зберігати навіть комбінацію з двох реквізитів (номер картки/строк дії Картки/ СVC2/CVV2) в менеджері паролів, чи іншому аналогу, що пропонує автоматичне внесення даних.

53. Якщо оплата товару (послуги) здійснюється через чужий комп’ютер, то рекомендуємо після завершення всіх розрахунків переконатися, що персональні дані та інша інформація не зберіглася (знову відкривши сторінку продавця, на якій здійснювалась оплата товару).

54. Слід встановити на свій комп’ютер антивірусне програмне забезпечення і регулярно здійснювати його оновлення та оновлення інших програмних продуктів (операційної системи, прикладних програм). Це захистить від проникнення шкідливого програмного забезпечення (вірусів).

55. Якщо вам надходять повідомлення з одноразовими паролями підтвердження операції, але Ви не проводили операцію розрахунку, негайно зверніться до Банку за телефонами Клієнтської підтримки 0800503434, +380443649828.

**V. Рекомендації Держателям платіжних карток Банку**

**щодо закриття поточного рахунку**

56. Пам’ятайте, що поточні рахунки закриваються на підставі заяви Клієнта, інших підставах, передбачених законодавством України або Договором між Банком і Клієнтом.

57. Якщо Ваша Картка видана Вам для одержання заробітної плати, у разі звільнення з роботи (або дострокового розірвання Договору з Вашої ініціативи), якщо не плануєте використовувати в подальшому рахунок, доцільно закрити поточний рахунок, який був відкритий для отримання заробітної плати. Для цього необхідно звернутися із заявою про закриття рахунку до Банку, і повернути Картку (у разі потреби), одержати довідку про закриття рахунку. Якщо ж маєте бажання продовжувати використовувати Картку, необхідно звернутися до Банку із заявою про зміну тарифного плану, відповідно якого буде обслуговуватися Картка. В будь-якому випадку, після отримання від роботодавця інформації про звільнення, тарифний план по Картці буде змінено.

58. При закритті поточного рахунку (після виконання зобов’язань або в разі розірвання чи закінчення терміну дії Договору) Банк виплачує кошти готівкою (у разі їх наявності) або за дорученням Клієнта переказує їх на інший рахунок.

59. Не рекомендуємо власноруч знищувати Картку (навіть якщо рахунок у Банку вже закрито). Це повинні робити (бажано у Вашій присутності) працівники Банку-емітента.