БАНК КЛІРИНГОВИЙ ДІМ

**Правила та поради з використання картки**

## Підрозділ 1. ПАМ'ЯТКА КЛІЄНТУ АБ «КЛІРИНГОВИЙ ДІМ»

(для уникнення незручностей при користуванні Карткою)

1.1. Запам'ятайте або занотуйте телефон цілодобової клієнтської підтримки Банку **0-800-50-18-08** або **+38 044 593-10-20.**

За цими телефонами Ви можете зв'язатися з Банком та отримати консультацію по Вашій Картці.

1.2. Запам'ятайте слово-пароль, яке Ви вказали при оформленні Картки! Слово-пароль буде необхідне для голосової авторизації при Вашому зверненні до Контакт центру Банку.

1.3. Зберігати ПІН-конверт потрібно окремо від Картки, в місці, яке відоме тільки Вам, і до якого не мають доступу інші особи, або запам'ятайте ПІН-код, а ПІН-конверт – знищіть (але не викидайте його цілим).

1.4. Не записуйте ПІН-код навіть у змінній формі на Картці або на інших, паперових носіях у відкритому вигляді.

1.5. Нікому не повідомляйте ПІН-код, навіть співробітникам Банку.

1.6. Завжди тримайте в полі зору Вашу Картку при обслуговуванні у торгово-сервісній мережі.

1.7. Не передавайте Вашу Картку або її реквізити іншим особам, в тому числі родичам, друзям, дітям.

1.8. У разі виявлення втрати Картки або підозри на її незаконне використання – заблокуйте її у мобільному додатку MyBank365 або за телефоном **0-800-50-18-08** або **+38 044 593-10-20**, та зверніться за перевипуском втраченої БПК.

1.9. Знання повного номеру Картки або останніх її чотирьох цифр прискорить операцію блокування вразі звернення за телефоном.

1.10. Розблокування Картки, яку було втрачено, або яка побувала у руках сторонніх осіб, підвищує ризик втрати коштів з Вашого КР та виникнення шахрайських операцій.

1.11. Пам'ятайте, розрахунок Карткою в мережі інтернет, підвищує ризик шахрайських операцій по Вашій Картці а в наслідок і втрати коштів з Вашого КР.

1.12. З метою недопущення несанкціонованого використання Ваших коштів (шахрайських операцій), рекомендуємо відмовитися від введення даних Картки (номер, строк дії, CVV2-код) на сайтах, що пропонують Вам участь у різноманітних акціях з виплатою бонусної винагороди, а також на інших підозрілих сайтах. Дані сайти спеціально створені для незаконного збору реквізитів БПК з метою подальшого шахрайського використання.

1.13. Встановлюйте ліміти на розрахунок Карткою в мережі інтернет.

1.14. Зверніть увагу! Банк ніколи не здійснює розсилання листів електронною поштою з проханням повідомити інформацію про Картку (номер, ПІН-код, строк дії та інше). Банк ніколи не вимагатиме введення на будь-яких сайтах таких параметрів Вашої Картки, як її номер, строк дії, CVV2-коду та ПІН-код. Необхідно ігнорувати та не відповідати на листи, які потребують введення певних параметрів Вашої Картки. В таких випадках слід НЕГАЙНО зв'язатись з Банком за телефоном **0-800-50-18-08** або **+38 044 593-10-20**.

1.15. Не записуйте та нікому не повідомляйте CVV2/-код. Введення CVV2 є підписом клієнта й прирівнюється до введення ПІН-коду при проведенні платіжної операцій в мережі Інтернет та/або платіжних операцій з ручним вводом даних Картки.

1.16. Щонайменше 1 раз на місяць отримуйте в банку контрольну виписку по КР або підключіться до послуги «СМС-інформування».

1.17. Не користуйтесь підозрілими банкоматами (на яких є предмети, залишки клею або інші сторонні пристрої, що викликають підозру).

1.18. З метою забезпечення безпеки операцій з використанням Вашої Картки, Банк інформує відносно ризику можливої компрометації Картки в нижченаведених країнах Індокитаю та Африки: Індонезія, , Китай, Малайзія, Сінгапур, Тайвань, , Шрі-Ланка, Філіппіни, Ангола, Ботсвана, Бурунді, Гана, Єгипет, Замбія, Кенія, Конго, Мозамбік, Намібія, Нігерія, Лівія, Сомалі, Чад, Ефіопія, тощо.

Дотримання цих правил забезпечить збереження Ваших коштів!

## Підрозділ 2. ПРАВИЛА КОРИСТУВАННЯ БАНКОМАТОМ

1.19. Банкомати обслуговують тільки ті Картки, логотипи яких вказано на корпусі або на екрані банкомату.

1.20. Переконайтесь, що банкомат працює – екран банкомату світиться та на ньому є привітання/перелік доступних номіналів банкнот/інформація про послуги, які надає Банк.

У випадку, якщо банкомат не працює, на екрані з'явиться повідомлення Банкомат тимчасово не працює/OFF LINE, або ж екран не буде "світитися" взагалі.

1.21. Переконайтесь, що до банкомату не приєднані сторонні пристрої, які викликають підозру: накладки на клавіатурі, додаткові екрани, схеми, чіпи і т.п..

1.22. Вставте Вашу Картку в приймальник банкомату (магнітна стрічка внизу - праворуч).

1.23. Оберіть мову спілкування з запропонованого переліку (українська, російська, англійська).

1.24. Введіть ПІН-код, підтвердіть його та продовжіть виконувати бажану платіжну операцію.

1.25. Повідомлення про введення невірного ПІН-коду Ви отримаєте лише після обрання бажаної платіжної операції. Вам буде запропоновано ввести ПІН-код ще раз.

1.26. У разі повідомлення про неправильне введення ПІН-коду уважно наберіть його ще раз. Якщо повідомлення про неправильне введення ПІН-коду з'явиться знову, значить Ви вводите неправильний ПІН-код. В разі трикратного невірного введення ПІН-коду на Картку автоматично встановлюється статус "Вилучити".

1.27. У держателів Карток АБ «КЛІРИНГОВИЙ ДІМ», доступна послуга розблокування Картки у випадку невірного введення ПІН-коду, для цього потрібно зателефонувати до Контакт-центру Банку.

1.28. «Затриману» Картку банкоматом не можливо повернути одразу. Звернувшись до Банку, Ви можете замовити перевипуск «затриманої» Картки (здійснюється згідно з тарифами Банку).

1.29. Оберіть операцію, яку Ви бажаєте виконати, з запропонованого переліку:

1.30. Зміна ПІН-коду – операція передбачена для зміни ПІН-коду по Вашій Картці у випадку втрати діючого (для зміни необхідно попередньо зателефонувати до Контакт-центру Банку або виконати функцію зміни ПІН-коду в Мобільному додатку) або якщо Вам не подобається діючий.

1.31. Міні-виписка – операція надає можливість отримати виписку по десяти останніх операцій, які виконувались Карткою: зняття готівки, покупки, інші витратні операції (поповнення Рахунку не відображаються).

1.32. СМС– операція надає змогу перевірити чи підключена Картка до послуги СМС-інформування та перевірити номер мобільного телефону, на який відправляються повідомлення.

1.33. Баланс – операція надає можливість отримати інформацію про залишок на Картковому рахунку (основний, накопичувальний – за вибором) у обраній валюті (Українська гривня, Долари США, Євро) та зручним способом (на екран банкомату або роздрукувати на чек).

1.34. Видача готівки – платіжна операція надає можливість отримати готівкові кошти з основного Карткового рахунку. Після вибору даної платіжної операції Вам буде запропоновано перелік сум, які можливо отримати, якщо жодна з сум Вас не задовольняє – оберіть пункт «Інша сума» та вкажіть потрібну суму за допомогою циферблату банкомату. При виборі суми слід пам'ятати, що за одну платіжну операцію банкомат може видати не більше 40 купюр. Якщо Вам потрібна велика сума готівки, спробуйте її отримати виконавши платіжну операцію «видача готівки» кілька разів. Після введення суми, у Вас є можливість обрати яким номіналом купюр отримати замовлену суму: «Дрібними», «Різними» або «Крупними».

1.35. Після проведення операції в банкоматі – заберіть Вашу Картку, отримайте готівку (якщо Ви замовили відповідну операцію) та отримайте чек. У випадку, якщо Ви не встигли забрати Картку чи готівку – вони будуть затримані та повернуті в банкомат (Картка буде затримана через 12 секунд, готівка – через 30 секунд).

## Підрозділ 3. ІНСТРУКЦІЯ З ВИКОРИСТАННЯ ПЛАТІЖНОЇ КАРТКИ В МЕРЕЖІ ІНТЕРНЕТ

В даному підрозділі Умов під мережею Інтернет маються на увазі всі різновиди програмно-технічних комплексів, в т. ч. застосунки, які надають змогу провести операцію оплати/попередньої оплати товарів/робіт/послуг шляхом введення реквізитів Карти (номер карти, термін дії та CVV).

1.36. Банківські платіжні картки класу Visa Bussines, Visa Platinum Business, які пропонує АБ «КЛІРИНГОВИЙ ДІМ», надають їх Держателям можливість проводити розрахунки в мережі Інтернет.

1.37. З метою мінімізації ризику виникнення шахрайських операцій з використанням даних Картки Держателя, АБ «КЛІРИНГОВИЙ ДІМ» встановлює ліміти (обмеження) на суму платіжних операцій, які можуть бути проведені за відповідною Карткою в мережі Інтернет. При оформленні Картки, первинні встановлені ліміти по даному виду платіжних операцій рівні «0», тобто Держатель не має можливість використовувати Картку в мережі Інтернет.

1.38. Держатель Картки має змогу за власним бажанням змінити стандарті ліміти на платіжні операції в мережі Інтернет в через Контакт центр банку (в телефонному режимі).

1.39. При встановлені ліміту для проведення в мережі Інтернет Держателю карти доступні постійно-діючі ліміти (добові та або місячні) та тимчасові ліміти (певна сума на певну кількість днів) Слід звернути увагу на те, що при здійсненні платіжних операцій в мережі Інтернет необхідно дотримуватися правил, які наведені нижче, щоб інформація про дані платіжних операції та реквізити Картки не стали відомі іншим особам і використані ними без згоди або з відома Клієнта/Банку, в внаслідок чого може бути завдано фінансової шкоди Держателю, за яку АБ «КЛІРИНГОВИЙ ДІМ» відповідальності не несе.

Всю відповідальність за здійснення даних платіжних операцій (без зчитування даних з Картки, в т.ч. в мережі Інтернет), в межах встановленого витратного ліміту, Держатель бере на себе.

При перевипуску Картки з якої-небудь причини, по якій встановлено витратний ліміт на платіжні операції в мережі Інтернет, встановлений витратний ліміт буде перенесений на нову Картку, обсяг встановленого розміру ліміту на новій Картці поновлюється в повному обсязі незалежно від часу та дня місяця.

1.40. При використанні Картки в мережі Інтернет важливо дотримуватися наступних правил безпеки:

1.40.1. Ніколи не висилати номер Картки через електронну пошту.

1.40.2. Переконатися, що компанія, якій здійснюється оплата товарів чи послуг, заслуговує на довіру і має хорошу репутацію.

1.40.3. Веб-сторінка, на якій необхідно ввести дані Картки повинна використовувати додатковий захист, тобто адресу сторінки повинен починатися так: https: // ****, де буква «s» вказує на захищений зв'язок.

1.41. Банк, у своїх електронних повідомленнях, ніколи не просить Держателя Картки надати про себе додаткову інформацію або ж перейти на іншу сторінку за наданим йому посиланням.

1.42. На гаджетах бажаним є використання програмного забезпечення, яке захищає його від вірусів і «хакерських» атак.

1.43. Після проведення платежу слід зберігати/роздрукувати отриманий чек за здійснену покупку.

1.44. Бажано уникати публічних місць (Інтернет кафе, кінотеатрів, місць відпочинку та ін.) при проведенні платежів.

1.45. У разі виникнення будь-яких підозр, щодо проведення шахрайських операцій з використанням Вашої Картки або ж підозр про можливість їх здійснення у зв'язку з можливим розголошенням конфіденційної інформації, слід негайно повідомити Банк звернувшись до Контакт центру або відділення Банку..

1.46. Порядок здійснення платежу за допомогою Картки в мережі Інтернет:

1.46.1. Детально ознайомитися з правилами та порядком проведення платежу, терміном доставки замовленого товару та умовами його повернення, у випадку, якщо товар не задовольнить Ваших вимог.

1.46.2. Перед проведенням платежу необхідно упевнитися в тому, що Вами надана коректна інформація щодо адреси доставки і Ваших контактних даних.

1.46.3. Знайти і заповнити поле, куди необхідно ввести номер Картки (16 цифр, які знаходяться на лицьовій стороні картки).

1.46.4. Знайти і заповнити поле, куди необхідно ввести дату закінчення терміну дії Картки (як правило, дата вноситься у форматі місяць/рік).

1.46.5. Знайти і заповнити поле, куди необхідно ввести CVV2 код (три останні цифри номера, який міститься на зворотному боці Картки на смузі для підпису).

1.46.6. У випадку, коли після проведення оплати Вам надається можливість роздрукувати документ, який підтверджує оплату, необхідно роздрукувати або зберегти наданий документ.

1.46.7. Після введення всіх даних Картки, які потрібні для здійснення оплати за товари або послуги, як правило, необхідно натиснути кнопку «Здійснити оплату»/«Оплатити» або іншу, яка підтверджує ваше бажання провести платіжну операцію. У цьому випадку слід звернути увагу на те, що після натискання кнопки «Оплатити» необхідно дочекатися підтвердження проведення платіжної операції і не натискати кнопку оплати двічі, так як в цьому випадку можливе здійснення подвійного списання коштів.

1.46.8. У випадку, якщо після проведення оплати Вам був наданий код підтвердження платіжної операції, цей код необхідно зберегти для того, щоб надалі Вашу оплату можна було ідентифікувати. У деяких випадках підтвердження здійснення платіжної операції надсилається на Вашу електронну адресу. У цьому випадку лист необхідно зберегти.

### Підрозділ 4. ЗАХИСТ ПРАВ КОРИСТУВАЧІВ ПЛАТІЖНИХ КАРТОК

1.47. Банк приймає Ваші звернення за телефонами Контакт-центру, електронною поштою, поштою або особисто (звернення у відділеннях Банку). Звернення до Контакт-центру приймаються цілодобово.

1.48. Ви маєте право звертатися до Національного банку України щодо вирішення порушених у зверненнях питань, включаючи випадки, якщо Банк не надав відповідь на звернення в установлений законодавством України термін для розгляду звернень або отримана відповідь Вас не задовольнила.

1.49. Банк завчасно, у строки визначені законодавством України, повідомить Вас про зміни тарифів та умов обслуговування.

1.50. Банк у своїй рекламі розкриває повну, точну та достовірну інформацію щодо послуг та Тарифів.

1.51. Банк розміщує на офіційному веб-сайті повну та достовірну інформацію щодо Тарифів, умов обслуговування та іншу інформацію визначену нормативними документами Національного банку України та законодавством України щодо захисту прав користувачів.

1.52. Банк не надає платіжні картки без відповідного запиту, крім випадку надання платіжних карток на заміну раніше виданих.

1.53. Всі розбіжності та спори, що виникають між Вами та Банком вирішуються шляхом переговорів. У випадку неможливості досягти згоди спір вирішується в судовому порядку згідно чинного законодавства України.

### Підрозділ 5. ВЗАЄМОДІЯ НА ВИПАДОК: ШАХРАЙСТВА (ПІДОЗРИ ШАХРАЙСТВА), ЗАГРОЗИ БЕЗПЕЦІ ВИКОНАННЯ ПЛАТІЖНОЇ ОПЕРАЦІЇ.

1.54. Банк забезпечує найвищий рівень безпеки платіжних операцій.

1.55. Банк здійснює моніторинг операцій з використанням платіжних карток або їх реквізитів.

1.56. Банк на постійній основі виявляє шахрайські схемі та вживає заходи для протидії їх реалізації.

1.57. Банк вживає заходів щодо оновлення версій програмного забезпечення і встановлює актуальні оновлення безпеки щодо усунення вразливості програмного забезпечення.

1.58. Банк реагує на підозрілі активності по картковим рахункам, для запобігання шахрайським операціям, використовує систему лімітування операцій, динамічні паролі, тощо.

1.59. Банк використовує технологію 3-D Secure[1] для підтвердження операцій під час операцій в через веб-сайти в інтернеті.

1.60. Банк співпрацює із ЄМА[2] для попередження виникненню шахрайських операцій.

## ПІДРОЗДІЛ 6. ВЗАЄМОДІЇ У РАЗІ ЗДІЙСНЕННЯ ПОМИЛКОВИХ, НЕНАЛЕЖНИХ ПЛАТІЖНИХ ОПЕРАЦІЙ.

1.61. У разі здійснення неналежних операцій з використанням платіжної картки або її реквізитів, заблокуйте картку у мобільному додатку MyBank365, повідомне Банк наступними шляхами:

– за телефонами Контакт-центра,
– особисто у відділеннях Банку.

1.62. Щодо відшкодування збитків у разі здійснення помилкових, неналежних платіжних операцій звертається до Банку наступними шляхами:

– за телефонами Контакт-центра,
– особисто у відділеннях Банку,
– електронною поштою,
– поштою.

1.63. Банк в обов'язковому порядку розглядає повідомлення помилкових або неналежних платіжних операцій, здійснених з використанням платіжних карток або їх реквізитів та надає можливість одержувати інформацію про хід розгляду повідомлення у строк та спосіб передбачений Законодавством України.

[1] 3-D Secure (три-де-сек'юр**)** - це протокол здійснення автентифікації держателя платіжної картки під час проведення операції в мережі інтернет шляхом введення Держателем одноразового цифрового пароля, що надійшов від Банку у СМС на зареєстрований номер телефону Держателя, який було вказано при укладанні Договору. Введення одноразового цифрового паролю в момент здійснення платіжної операції в мережі Інтернет держатель підтверджує участь та згоду на проведення такої платіжної операції.

[2] ЄМА - Українська міжбанківська Асоціація членів платіжних систем «ЄМА».