

Витяг
з Положення про відкритий банкінг в акціонерному товаристві
"Полікомбанк"
(затверджене рішенням Правління банку від 23.07.2026, протокол № 32)

"11. Порядок взаємодії Банку та НПП з ініціювання щодо здійснення неакцептованих, помилкових та неналежних платіжних операцій та порядок відшкодування збитків користувачу, завданих в результаті проведення таких платіжних операцій"

11.1. Порядок взаємодії між Банком та НПП з ініціювання у випадку здійснення неакцептованих, помилкових, неналежних платіжних операцій (в тому числі з використанням платіжної інструкції) – відповідає загальній процедурі взаємодії з користувачем, з урахуванням наступного:

1) звернення НПП з ініціювання та/або користувача щодо випадку здійснення неакцептованих, помилкових, неналежних платіжних операцій розглядається відповідальним працівником Банку, який обслуговує цього користувача та начальником сектору інформаційної безпеки, або інший уповноважений працівник Банку, який має відповідний фах, компетенцію та досвід у сфері інформаційної безпеки;

2) звернення щодо випадку здійснення неакцептованих, помилкових, неналежних платіжних операцій розглядається Банком протягом 15 календарних днів, а про результати розгляду та прийняті рішення НПП з ініціювання повідомляється не пізніше 15 днів;

3) у разі необхідності повідомлення користувача або НПП з ініціювання про випадок здійснення з його рахунку неакцептованих, помилкових, неналежних платіжних операцій, він повідомляється невідкладно, а для передачі повідомлення використовується будь-який наявний спосіб зв'язку;

4) за результатами проведення відповідного розслідування щодо обставин здійснення неакцептованої, помилкової, неналежної платіжної операції, Банк не пізніше 15 днів надає користувачу інформацію у відповідному обсязі, включаючи відомості про факт отримання згоди користувача, застосовані процедури автентифікації та передані до Банку платіжні інструкції;

5) в разі незгоди з Банком, користувач подає письмову заяву щодо відшкодування збитків, складену у довільній формі та підписану у звичайний спосіб або за допомогою електронного підпису в разі подання заяви в електронному вигляді;

6) особливості порядку розгляду звернень користувача за неналежними та помилковими платіжними операціями, а також порядку повернення йому коштів за такими операціями – викладено у договорі на обслуговування його рахунку;

7) Банк приймає всіх можливих заходів у цілодобовому режимі без вихідних, для забезпечення взаємодії з НПП з ініціювання на випадок здійснення неакцептованих, помилкових, неналежних платіжних операцій.

11.2. Банк не несе відповідальності, якщо платіжна операція виконана Банком належним чином.

11.3. В разі встановлення Банком факту його вини, він відшкодовує нанесені користувачу збитки, завдані в результаті проведення неакцептованих, неналежних, помилкових платіжних операцій у строк не більше 3 банківських днів, з моменту встановлення факту вини.

Під збитками розуміються понесені користувачем збитки за встановленої вини Банку.

11.4. В разі невстановлення факту наявності вини Банку за результатами внутрішнього розслідування— Банк пропонує НПП з ініціювання інші способи врегулювання спорів.

11.5. Банк щоденно проводить моніторинг здійснених платіжних операцій через сторонніх НПП за параметрами, встановленими правилами платіжної системи, з метою ідентифікації помилкових та неналежних, суб'єктів цих платіжних операцій та вжиття заходів із запобігання або їх припинення.

13. Порядок дій Банку на випадок шахрайства (підозри шахрайства) або загрози безпеці виконання платіжної операції, ініційованої користувачем та/або надання відомостей з його рахунків

13.1. Банк забезпечує постійний моніторинг операцій, запитів на доступ до рахунків користувачів та функціонування спеціалізованих інтерфейсів відкритого банкінгу з метою своєчасного виявлення ознак шахрайства, підозрілої активності, несанкціонованого доступу або інших загроз безпеці виконання платіжних операцій та надання відомостей з рахунків користувачів.

13.2. Підставами для застосування заходів реагування можуть бути:

- 1) виявлення ознак несанкціонованого доступу до рахунку користувача;
- 2) виявлення ознак компрометації засобів автентифікації користувача;
- 3) надходження інформації про можливе шахрайство від користувача, стороннього НПП, інших надавачів платіжних послуг, правоохоронних органів або уповноважених державних органів;
- 4) виявлення аномальної або нетипової активності під час ініціювання платіжної операції чи доступу до відомостей з рахунку;
- 5) інші обставини, що можуть свідчити про загрозу безпеці користувача, Банку або учасників відкритого банкінгу.

13.3. У випадках шахрайства (підозри шахрайства), загрози безпеці виконання платіжної операції або неакцептованих, помилкових, неналежних платіжних операцій, ініційованої користувачем через НПП та/або надання відомостей з рахунків користувача через НПП, Банк під час розгляду звернення звертається до стороннього НПП з вимогою отримання інформації щодо наданої таким стороннім НПП нефінансової платіжної послуги користувачу у такому порядку:

- 1) запитує у стороннього НПП усю необхідну інформацію щодо ініціювання платіжної операції та/або ініціювання згоди/ запитів на отримання відомостей з рахунків шляхом направлення запиту на публічну корпоративну електронну пошту такого НПП;
- 2) очікує відповідь від стороннього НПП у строк до 3х робочих днів. Якщо відповідь не отримано у зазначений строк Банк може звернутися до НБУ із скаргою щодо роботи такого НПП;

3) у разі звернення НПП до Банку – Банк опрацьовує таке звернення протягом 5-ти робочих днів з дати отримання такого звернення;

4) у випадку загрози безпеки, виконання платіжної операції регулюється внутрішньою інструкцією та планом реагування інформаційної безпеки. Взаємодія у випадках шахрайства (підозри шахрайства), неакцептованих, неналежних платіжних операцій регламентується внутрішнім нормативним документом Банку.

13.4. Порядок взаємодії між Банком та НПП з ініціювання та/або користувачем у випадку шахрайства (підозри шахрайства) або загрози безпеці виконання платіжної операції – відповідає загальній процедурі взаємодії з користувачем, з урахуванням наступного:

1) звернення НПП з ініціювання та/або користувачем щодо випадку шахрайства або загрози безпеці розглядається сектором інформаційної безпеки негайно після його отримання;

2) про результати розгляду та прийняті рішення користувач повідомляється невідкладно, а для передачі повідомлення використовується будь-який наявний спосіб зв'язку;

13.5. Взаємодія між Банком та користувачем на випадок шахрайства (підозри шахрайства) або загрози безпеці відкритого банкінгу передбачає обов'язок Банку брати участь у розслідуванні обставин несанкціонованого доступу до рахунку користувача, неакцептованих або неналежно виконаних платіжних операцій, неправомірного отримання відомостей з рахунків користувача, а також інших випадків, що можуть свідчити про шахрайство або порушення вимог безпеки. Банк надає користувачу інформацію, що може бути розкрита відповідно до законодавства України та необхідна для розслідування зазначених випадків.

13.6. Банк має право без попереднього погодження з користувачем:

1) повідомляти сторонніх НПП, інших надавачів платіжних послуг, платіжні системи, Національний банк України та інші уповноважені органи про виявлені ознаки шахрайства, несанкціонованого доступу або інші події, що можуть створювати загрозу безпеці відкритого банкінгу;

2) тимчасово обмежити або припинити доступ стороннього НПП до спеціалізованого інтерфейсу Банку, зупинити виконання платіжної операції або надання відомостей з рахунку користувача у разі наявності обґрунтованої підозри щодо шахрайства, несанкціонованого доступу, компрометації засобів автентифікації чи іншої загрози безпеці;

3) вимагати проведення додаткової автентифікації користувача або додаткового підтвердження правомірності запиту на доступ до рахунку чи ініціювання платіжної операції.

13.7. У договорі на обслуговування рахунку користувача повинно бути передбачено обов'язок користувача невідкладно повідомляти Банк про:

1) відомі йому факти або підозри щодо шахрайських дій, пов'язаних із використанням сервісів відкритого банкінгу;

2) виявлення несанкціонованих платіжних операцій або запитів щодо отримання інформації з його рахунків;

3) компрометацію засобів автентифікації, облікових даних або інших засобів доступу до сервісів відкритого банкінгу;

4) будь-які обставини, які можуть свідчити про загрозу безпеці його рахунків або персональних даних.

13.8. У разі виявлення шахрайської операції, підозри щодо її здійснення, несанкціонованого доступу до рахунку, неправомірного отримання відомостей з рахунку або іншої загрози безпеці відкритого банкінгу користувач зобов'язаний невідкладно повідомити про це Банк через визначені Банком канали зв'язку та надати всю наявну інформацію, необхідну для перевірки обставин інциденту, вжиття заходів реагування та проведення розслідування. "