Вих. №12-04/3 (9)-16

від 12.09.2016р.

Щодо посилення контролю банків за комерційними агентами та доцільності врахування змін до Постанови № 705, що не було враховано Постановою № 382

ДИРЕКТОРУ ДЕПАРТАМЕНТУ ПЛАТІЖНИХ СИСТЕМ ТА ІННОВАЦІЙНОГО РОЗВИТКУ

ШАЦЬКОМУ С. С.

Шановний Сергію Сергійовичу!

Від імені банків членів платіжних систем бажаємо плідної роботи з реформування фінансового сектору України для підвищення довіри громадян до дій урядовців та фінансистів.

Щиро дякуємо за враховані Постановою Правління НБУ № 382 від 06 вересня 2016 року пропозиції членів платіжних систем до Проекту постанови Правління Національного банку України "Про внесення змін до Положення про порядок емісії електронних платіжних засобів і здійснення операцій з їх використанням".

Вимушені звернути Вашу увагу, на те, що окремі з пропозицій до Постанови № 705 було внесено у редакції, суттєво відмінній від запропонованої, а більшість пропозицій не було враховано взагалі, що у сукупності не зовсім позитивно впливає на правове становище кінцевого споживача – користувача платіжної послуги.

В тому числі, нами пропонувалося:

1. додати терміни наступного змісту, розділити та термінологічно окреслити у часових рамках значення слова “негайно”.

“Негайне повідомлення користувачем банку — дія, передбачена Законом, яка збігається з моментом прийняття користувачем рішення про підтвердження вказаного юридичного обов’язку та відбувається в порядку передбаченому

Договором одразу після отримання користувачем повідомлення банку про здійснену операцію з використанням електронного платіжного засобу користувача або виявлення ним факту втрати електронного платіжного засобу.

Негайне зупинення здійснення операцій з використанням електронного платіжного засобу - дія, передбачена Законом, яка збігається з моментом прийняття банком рішення про підтвердження вказаного юридичного обов'язку та відбувається в порядку передбаченому Договором одразу після отримання банком повідомлення користувача про втрату електронного платіжного засобу та/або платіжні операції, які не виконувалися користувачем."

Прийнята ж редакція Постанови №382 зафіксувала наступне визначення: "**негайно** – найкоротший строк протягом робочого дня, у який мають здійснюватися (відбуватися) відповідні дії, з моменту настання підстав для їх здійснення".

З точку зору розгляду спірних ситуацій та заяв користувачів, таке визначення загалом ускладнює як правове становище банка при проведенні ним службового розслідування та встановлення обставин (не)правомірності переказу, так і клієнта, що оспорює ту чи іншу операцію, оскільки воно конкретно не описує часові рамки та надає обом "запас часу" та поле для маніпуляцій проміжком у тривалість робочого дня, а у разі, якщо неправомірна дія та повідомлення про неї стались не у робочий час – до 24 годин.

Це зі свого боку вже на нормативному рівні стимулюватиме внутрішнє шахрайство співробітників банків та спонукатиме намагання до вчинення клієнтами неправомірних дій, а також наявність суперечливої судової практики.

З огляду на це, пропонуємо чітко термінологічно розмежувати "негайно" для користувача та "негайно" для банку у початково запропонованій редакції. Таким чином буде суттєво покращено правовий статус користувача платіжних послуг та обслуговуючого його банку.

Постановою № 382 було введено положення про "неможливість включення до договору вимоги про безумовну відповідальність користувача ЕПЗ за неналежний переказ, за винятком, якщо доведено, що дії чи бездіяльність користувача призвели до втрати ЕПЗ, розголошення ПІНу або іншої інформації, що дає змогу ініціювати платіжну операцію".

Утім, більшість інших пропозицій, що стосуються безпеки здійснення платіжних операцій та управління ризиками не було враховано. У зв'язку з цим, звертаємося до Вас повторно з пропозицією включити в текст Постанови наступні доповнення, зважаючи на нижченаведені аргументи.

Ми пропонуємо:

2. підпункт 10) пункту 8 Розділу II. Емісія електронних платіжних засобів викласти в наступній редакції:

“10) право банку на час встановлення правомірності переказу:

- зупиняти зарахування коштів на рахунок користувача у разі надходження від банку-ініціатора повідомлення про неналежний переказ коштів;

- забороняти видаткові операції по рахунку на суму помилкового або неналежного переказу або встановлювати ліміт по рахунку та/або за електронним платіжним засобом та/або на певні типи (види) операцій”;

Запропонована норма є важливою та необхідною частиною механізму повернення коштів у разі здійснення помилкового або неналежного переказу, - насамперед при здійсненні переказів з картки на картку.

Включення цієї норми до тексту Постанови, слугуватиме послідовним кроком НБУ на виконання раніше наданих рекомендацій банкам щодо можливості використання механізму договірного списання в якості нормативного підґрунтя, яке наразі, на жаль, досі відсутнє на рівні підзаконного акту.

3. додати підпункт 10.1) в пункту 8 Розділу II. Емісія електронних платіжних засобів та викласти в наступній редакції:

“10.1) право банку на списання коштів з рахунку користувача без його розпорядження, у разі надходження від банку ініціатора платежу повідомлення про помилковий або неналежний переказ коштів з рахунку платника”;

Запропонована норма також є важливою та **необхідною частиною механізму повернення коштів** у разі здійснення помилкового або неналежного переказу, - насамперед при здійсненні переказів з картки на картку.

4. абзац третій пункту 2 Розділу VI. Загальні вимоги до безпеки здійснення платіжних операцій та управління ризиками викласти в наступній редакції:

“Користувач зобов'язаний надійно зберігати та не передавати іншим особам електронний платіжний засіб, ПІН, інші засоби, які дають змогу користуватися

ним, у тому числі унікальний ідентифікатор, повідомлений банком користувачу, який повинен бути наданий ним з метою забезпечення ідентифікації користувача при виконанні платіжної операції";

Наведене уточнення є необхідним з огляду на динамічний розвиток технологічного аспекту переказу коштів в Україні, й зокрема стосується запровадження та активного використання двохфакторної аутентифікації, технології 3D-Secure тощо, та важливості нормативного захисту усіх елементів, що застосовуються у цілях забезпечення схоронності персоналізованих засобів безпеки при здійсненні платіжної операції.

5. додати підпункт 4) в пункт 1 Розділу VI. Загальні вимоги до безпеки здійснення платіжних операцій та управління ризиками викласти в наступній редакції:

"Основними способами інформування (повідомлення) користувача, які банк повинен йому запропонувати, є SMS інформування та/або емейл інформування. До додаткових способів інформування користувача відноситься інформування за допомогою Месенджеру, USSD додатку, додатку для Push-повідомлень. Банк та користувач відповідно до умов договору можуть домовитись про інші прийнятні для них додаткові способи інформування, отримання повідомлень, а також про основні (додаткові) способи інформування, отримання повідомлень про що зазначено в Договорі".

Наведене уточнення є необхідним з огляду на динамічний розвиток інформаційних технологій та новітніх засобів комунікації в Україні та практики, що є застосовуваною, прийнятною та бажаною з точки зору побудови бізнес процесів у банках при інформуванні клієнтів. **Зазначена норма розширює можливості для банку та користувача і забезпечує право користувача на вільний вибір способу такого інформування та багатоманітність його каналів**, виходячи із міркувань зручності та економічної доцільності надаваної послуги для кінцевого споживача, що фіксується за принципом "свободи договору" між ним та банком.

6. додати абзац п'ять до пункту 4 Розділу VI. Загальні вимоги до безпеки здійснення платіжних операцій та управління ризиками та викласти його в наступній редакції:

"Обов'язкова інформація, надана користувачем банку для здійснення контактів, має включати номер мобільного телефону та /або адресу електронної скриньки користувача".

Стаття 14 ЗУ “Про платіжні системи та переказ грошей в Україні” передбачає обов’язковою умовою виконання банком вимог з інформування відповідний обов’язок користувача надати (та оновлювати) контакту інформацію, з використанням якої інформування може бути здійснено. Найбільш поширеним у світі і Україні (фактично стандартним) засобом комунікації громадян є мобільний зв’язок та електронна пошта. Саме тому для роз’яснення вимог Закону та забезпечення практичної реалізації права громадян на інформування та обов’язку банку здійснювати інформування належним чином на поточному етапі розвитку ринку потрібне доповнення та уточнення зазначеного питання.

7. додати абзац три до пункту 6 Розділу VI. Загальні вимоги до безпеки здійснення платіжних операцій та управління ризиками та викласти його в наступній редакції:

“Банк та клієнт можуть домовитись про граничний термін, протягом якого користувач має зробити негайне повідомлення, але зазначений термін не може перевищувати 1 години”.

Зазначена норма є невід’ємною частиною механізму з пропозиції №1 та **направлена на максимальне убезпечення схоронності коштів на банківському рахунку клієнта та мінімізацію ризиків збитків**, але, з урахуванням принципу розумності, обумовлює можливість встановлення у договірному порядку певних виключень з нього (наприклад, шляхом повідомлення клієнтом банку за встановленою процедурою вимоги про необхідність відхилення від такого правила з урахуванням відсутності клієнта протягом певного часу у межах країни або зоні дії мобільного зв’язку тощо, у зв’язку з чим клієнт звертається до банку з проханням не застосовувати певний час це правило, а посилити інші засоби забезпечення схоронності його коштів – такі як ліміти тощо).

8. додати абзаци три - п’ять до пункту 7 Розділу VI. Загальні вимоги до безпеки здійснення платіжних операцій та управління ризиками та викласти їх в наступній редакції:

“Термін, протягом якого банк зобов’язаний негайно зупинити здійснення операцій з використанням цього електронного платіжного засобу не може перевищувати 10 хвилин з моменту фіксації обставин заяви, дати, години та хвилини його звернення.

При цьому ризик збитків від здійснення операцій за електронним платіжним засобом користувача банк несе з моменту фіксації обставин заяви, дати, години та хвилини його звернення.

Емітент має право передбачити в Договорі зобов'язання користувача підтвердити його заяву письмово та надати докази звернення користувача до правоохоронних органів".

Зазначена норма є невід'ємною частиною механізму з пропозиції №1 та направлена **на максимальне убезпечення схоронності коштів на банківському рахунку клієнта та мінімізацію ризиків його збитків**. Фіксації звернення клієнта та зведення до мінімуму часового проміжку з моменту звернення до моменту блокування рахунку є реальним дієвим способом, що дасть змогу не втрачати час при здійсненні та встановленні факту неправомірного переказу з метою зупинення та повернення неналежно або помилково списаних коштів з рахунку належного користувача, що вчинив усі необхідні дії для збереження коштів та негайно повідомив банк про списання коштів з його рахунку за операцією, що він не здійснював.

9. додати абзац два до пункту 8 Розділу VI. Загальні вимоги до безпеки здійснення платіжних операцій та управління ризиками та викласти їх в наступній редакції:

"Видаткові операції по рахунку на суму помилкового або неналежного переказу дозволяються користувачу емітентом в разів встановлення емітентом не правомірності переказу та в строки встановлені Законом".

Зазначена пропозиція дозволяє практично захищати інтереси користувачів, шляхом **створення умов, які унеможливлюють виведення коштів з банківських рахунків шахраїв** та спрощують можливості банку отримувача відшкодування коштів особам, з рахунків яких кошти було неправомірно списані в іншому банку.

10. пункт 9 Розділу VI. Загальні вимоги до безпеки здійснення платіжних операцій та управління ризиками викласти в наступній редакції:

"Користувач не несе відповідальності за здійснення платіжних операцій, якщо електронний платіжний засіб було використано без фізичного пред'явлення користувачем та/або електронної ідентифікації самого електронного платіжного засобу і його користувача, крім випадків, якщо користувачем доведено, що його дії чи бездіяльність не призвели до втрати, незаконного використання ПІНу або іншої інформації, яка дає змогу ініціювати платіжні операції, у тому числі унікального ідентифікатору, повідомленого банком користувачу, який повинен бути наданий користувачем з метою забезпечення його ідентифікації при виконанні платіжної операції";

Наведене уточнення є необхідним з огляду на активне використання двохфакторної аутентифікації та **численних фактів розголошення користувачами одноразових паролів**, наданих ним в процесі проведення аутентифікації.

Враховуючи вищезазначене, просимо Вас включити до Постанови №705 наші десять пропозицій та врахувати їх в максимально повному обсязі, або в разі не можливості їх врахування надати мотивовану відповідь щодо причин.

Додатково, просимо надати роз'яснення по листу Національного банку України від 07.09.2016 №57-002\75124 "Про посилення контролю банків за комерційними агентами".

З огляду на недостатній ступінь конкретизації у листі заходів, що вкладаються у поняття та маються на увазі під посиленням контролю з боку банків за комерційними агентами, просимо роз'яснити наступне:

1) Чи передбачав Національний банк, банки, які працюють з використанням агентської мережі, що обслуговує Webmoney, PerfectMoney, "Яндекс.Деньги" тощо з моменту отримання листа мають негайно припинити договірні та/або будь-які фактичні відносини з зазначеними агентами?

2) Якщо ні, просимо Національний банк роз'яснити, яким чином організаційно та технологічно банкам необхідно виконати зазначений припис

3) Чи означає наведене у листі те, що банки з моменту отримання листа зобов'язані заборонити поповнювати електронні гаманці зазначених систем через, або з використанням власної інфраструктури банку (банкомати, ПТКС, інтернет-банкінг тощо)?

4) Якщо так, просимо Національний банк роз'яснити, яким чином організаційно та технологічно банкам необхідно виконати зазначений припис?

З повагою,

Директор Карпов О.О.

Вик. Губська Д.О. (044) 568-58-38