

Юніна Марина Петрівна

доцент кафедри цивільного права та процесу
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук

ЗЛОЧИНИ З ВИКОРИСТАННЯМ БАНКІВСЬКИХ ПЛАТІЖНИХ КАРТОК ТА МОЖЛИВІ МЕТОДИ ЇХ ПОПЕРЕДЖЕННЯ ТА ПРОТИДІЇ

У сучасних соціально-економічних умовах розвиток комп'ютерних технологій та використання мережі Інтернет, яка стає найбільш розповсюдженим засобом комунікації у суспільстві, спричиняють появу нових видів злочинів. Особливою мірою це стосується сфери надання банківських послуг, зокрема, використання банківських карток. Найчастіше метою таких злочинів є отримання конфіденційної інформації про реквізити банківської картки і грошові кошти її власника та використання такої інформації для власного збагачення.

Стрімкий розвиток сфери банківських послуг, зокрема, розповсюдження банківських платіжних карток, призводить до збільшення кількості злочинів у цій сфері, а також до появи нових їх видів.

Одним з таких злочинів із використанням банківських платіжних карток наразі є так званий фішинг (від англійського fish – ловити рибу). Сутність таких дій полягає у вивідуванні у власника картки інформації, яка б допомогла злочинцю зняти з неї кошти. Це може бути лист-підробка на електронну пошту від імені банку-емітента платіжної картки або від сайту, де власник картки планував здійснити покупку, розплатившись картою, з проханням повідомити інформацію, за допомогою якої шахраї зможуть отримати доступ до коштів на картці (наприклад, PIN-код, строк дії картки, логін, пароль тощо). В цьому листі пропонується перейти за вказаним посиланням на сайт-клон, адреса якого відрізняється від справжньої адреси сайту банку чи сайту, що пропонує товари та послуги, на один або декілька символів. Якщо власник картки перейде за посиланням та введе реквізити картки, які вимагаються в листі, це дасть можливість злочинцям отримати інформацію, яка необхідна для заволодіння грошовими коштами власника картки [1].

Також досить відомим видом злочинів у сфері банківських послуг є скімінг, сутність якого полягає в тому, що на банкомат встановлюється спеціальна накладка-скімер, яка зчитує інформацію з магнітних смуг карток. Отримана інформація наноситься на підроблену картку, за допомогою якої з рахунка власника справжньої картки вилучаються кошти або підроблена картка використовується злочинцями для розрахунків за товари та послуги [4].

До найбільш розповсюджених злочинів у цій сфері вчені відносять також й вішинг (від англійського voice (голос) + fishing (ловити рибу)). Для да-

ного типу шахрайства характерними є дзвінки від начебто працівників банку, який випустив платіжну картку, з попередженнями про блокування картки, наприклад, за переказ грошей на картку від юридичної особи, прострочений платіж за кредитним договором, та необхідністю надати для її розблокування конфіденційну інформацію про картку, коди доступу та строк дії. Отримання даної інформації дозволяє злочинцям зняти грошові кошти, що знаходяться на банківському рахунку власника картки.

Наведений перелік злочинів із використанням банківських платіжних карток не є вичерпним. Створення та використання нових електронних платіжних документів сприяють появі нових видів таких злочинів та їх збільшенню у загальній кількості вчинюваних злочинів. Так, за даними Української міжбанківської Асоціації членів платіжних систем, найбільш розповсюдженими злочинами з використанням банківських карток є створення фішингових сайтів, вішинг та вірусні розсилки [9]. Лише за один рік вказаними злочинами спричиняється шкода на суму понад 500 млн. грн. [6]. При цьому протягом лише одного півріччя 2016 року було виявлено 117 фішингових сайтів, що у три рази більше, ніж за увесь попередній рік [8].

На жаль, органи Національної поліції стикаються з певними складнощами при розслідуванні вказаних злочинів, однією з яких є високий рівень їх латентності. Це пов'язано, насамперед, з правовою необізнаністю та фінансовою неграмотністю населення, а також з тим, що самі банки не завжди вчасно звертаються до правоохоронних органів, вважаючи, що їх втручання в розслідування такого виду злочинів зашкодить репутації банку [5, с. 84].

Зважаючи на вказані складнощі та усе більше розповсюдження злочинів з використанням банківських карток, на наш погляд, наразі є необхідним створення ефективних механізмів попередження та протидії таким злочинам. Зокрема, це може бути застосування додаткових механізмів технічного захисту інформації, яка зберігається на банківських платіжних картках. До таких механізмів відносять використання чип-модулів на банківських платіжних картках. Спеціалісти стверджують, що банківські картки з чипами є більш захищеними у порівнянні зі звичайними платіжними картками та мають найбільший рівень захисту інформації від шахрайських операцій [2, с. 30].

Також ефективним механізмом захисту від шахрайства з банківськими картками є підключення власником картки послуги 3-D Secure (прив'язка карти до номера мобільного телефону її власника, тобто проведення оплати буде здійснюватися лише після того, як власник картки підтвердить транзакцію шляхом введення коду, отриманого в смс-повідомленні).

Роз'яснювальна робота серед власників банківських карток щодо правил безпеки використання карток та зберігання конфіденційної інформації (наприклад, щодо строку дії картки, CVV-коду картки, PIN-коду картки, своєчасного повідомлення банку про крадіжку картки або її блокування тощо), що проводиться працівниками банків та правоохоронних органів, також є дієвим способом захисту від досліджуваних видів злочинів.

До основних способів запобігання вчиненню таких злочинів з боку від-

повідних державних органів можна віднести удосконалення нормативно-правового регулювання з питань забезпечення безпеки банківської системи з врахуванням позитивного міжнародного досвіду в боротьбі зі злочинами у сфері банківських послуг та запровадження більш досконалих технологій захисту у банківській сфері [5, с. 85].

Таким чином, можна зробити висновок про те, що сьогодні злочини у сфері надання банківських послуг стають усе більш розповсюдженими, з кожним роком від них потерпає усе більша кількість людей. Саме тому з урахуванням вимог сьогодення активізація роботи, спрямованої на попередження таких злочинів, удосконалення механізму протидії таким видам шахрайства, збільшення обсягів відповідальності за них стає нагальною потребою.

Разом з тим необхідно також зауважити, що безпека операцій, які проводяться за допомогою банківських платіжних карток, багато в чому залежить і від їх власників. Так, саме власнику картки необхідно потурбуватися про збереження конфіденційної інформації щодо картки, зокрема, не вчиняти дій, які б сприяли зловмисникам в отриманні та використанні такої інформації.

1. Абрамов К. Інтернет-шахрайство з платіжними картками та методи захисту від нього / К. Абрамов // Україна фінансова. Інформаційно-аналітичний портал Українського агентства фінансового розвитку [Електронний ресурс]. – Режим доступу : http://www.ufin.com.ua/analit_mat/poradnyk/094.htm.

2. Біломістна І.І. Сучасні тенденції розвитку ринку банківських платіжних карток в Україні / І.І. Біломістна // Економічні науки. – 2012. – № 9. – С. 26–36.

3. Григораш А. Обережно, шахраї. Як кіберзлочинці виманюють гроші українців / А. Григораш // Українська правда від 29.04.2013 р. – [Електронний ресурс]. – Режим доступу: <http://life.pravda.com.ua/society/2013/04/29/127670/>.

4. Гриньков Д. Шахрайство з платіжними картками та протидія йому в сучасних умовах / Д. Гриньков // Україна фінансова. Інформаційно-аналітичний портал Українського агентства фінансового розвитку [Електронний ресурс]. – Режим доступу: http://www.ufin.com.ua/analit_mat/poradnyk/191.htm.

5. Клочко А.М. Шахрайство з використанням банківських платіжних карток / А.М. Клочко, А.О. Єременко // Юридичний науковий електронний журнал. – 2016. – № 1. – С. 82–86 [Електронний ресурс]. – Режим доступу: http://lsey.org.ua/1_2016/23.pdf.

6. МВС розкрило статистику збитків через шахрайство з банківськими картками в Україні [Електронний ресурс]. – Режим доступу: <http://biz.nv.ua/ukr/finance/mvs-rozkrilo-statistiku-zbitkiv-z-za-kartkovogo-shahrajstva-v-ukrajini-68143.html>.

7. Про затвердження Правил Національної системи масових електронних платежів : постанова Правління Національного банку України від 10.12.2004 р. № 620 [Електронний ресурс]. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/z0025-05>

8. Рост фішинга достиг 300 % в год. Новые данные в докладе ЕМА Academy [Електронний ресурс]. – Режим доступу: <https://ema.com.ua/ema-ii-international-conference-payment-systems-and-financial-markets/>.

9. Українська міжбанківська Асоціація членів платіжних систем [Електронний ресурс]. – Режим доступу: <https://ema.com.ua/>.