

УДК 343.72

Заріцька О. С., викладач, спеціаліст вищої категорії, Вишнянський коледж Львівського національного аграрного університету, м. Львів.

Коцан-Олинець Ю. Я., доцент кафедри теорії держави та філософії права Львівського національного університету імені Івана Франка

ВИДИ ШАХРАЙСТВА З БАНКІВСЬКИМИ КАРТКАМИ ТА СПОСОБИ ПРОТИДІЇ ЇХ ПРОЯВАМ

Анотація. У статті аналізується сучасний стан шахрайства, вчиненого з використанням банківських платіжних карток, обґрунтовується необхідність вдосконалення способів протидії його проявам в сучасних умовах.

Подана коротка характеристика основних видів шахрайства з банківськими картками. Пропонуються можливі напрями роботи із запобігання вчиненню злочинів пов'язаних із шахрайськими діями в банківській системі.

Автори дійшли висновку, що шахрайство з банківськими картками має значні негативні наслідки для стабільності фінансової системи, оскільки гальмує поширення безготівкової форми оплати, яка є визнаним пріоритетом розвитку світової фінансової системи. За результатами дослідження пропонуються обґрунтовані першочергові заходи щодо запобігання вчиненню злочинів пов'язаних із шахрайськими діями в банківській системі слід віднести.

Ключові слова: банківська платіжна картка, шахрайство з банківськими картками, види шахрайства, способи протидії проявам шахрайства, злочини.

Zaritska O. S., teacher, specialist of the higher category of Vyshnya College of Lviv National Agrarian University, Lviv.

Kotsan-Olinets U. Ya., Associate Professor of the Department of State Theory and Philosophy of Law, Ivan Franko National University of Lviv

TYPES OF FRAUD WITH BANKING CARDS AND WAYS TO COUNTERACT ITS MANIFESTATIONS

Abstract. The article analyzes the current state of fraud committed with the use of bank payment cards, justifies the need to improve ways to counteract its manifestations in modern conditions.

A brief description of the main types of fraud with bank cards is given. Possible ways of preventing crimes connected with fraudulent actions in the banking system are offered.

The authors concluded that fraud with bank cards has significant negative consequences for the stability of the financial system, since it impedes the proliferation of cashless forms of payment, which is a recognized priority of the development of the world financial system. According to the results of the study, it is suggested that justified priority measures to prevent the commission of crimes related to fraudulent actions in the banking system should be considered.

Key words: a bank payment card, a bank card fraud, types of fraud, the methods of counteracting fraud, a crime.

JEL: K 14.

DOI: <https://doi.org/10.36477/2616-7611-2019-08-10>

Постановка проблеми. Перехід на безготівкову оплату з використанням банківських карток допомагають зробити сферу підприємницької діяльності максимально прозорою як для споживача, так і для продавця. У свою чергу розповсюдження даного виду платіжного засобу є також результатом діяльності держави, спрямованої на поступове обмеження операцій із готівковими платежами. Водночас із зростанням популярності розрахунків через банківські картки збільшується і кількість шахрайських спроб використання даних картокових користувачів для незаконного збагачення. Банківські установи також зазнають значної шкоди від таких дій, адже несуть певну відповідальність при здійсненні операцій за допомогою платіжної картки. Тому, зважаючи на викладене, науковий аналіз основних напрямів протидії шахрайствам із використанням банківських платіжних карток є надзвичайно актуальним та важливим в умовах розвитку інформаційних технологій в банківському секторі.

Аналіз досліджень даної проблеми. Проблему злочинних дій з використанням банківських платіжних карток досліджували у своїх працях як зарубіжні, так і вітчизняні вчені, такі, як: Л. В. Бистров, О. В. Курман, Г. А. Матусовський, С. І. Ніколаюк, С. В. Поперешняк, А. В. Реуцький, Т. В. Романенко, С. В. Самойлов, Л. М. Стрельбицька, О. В. Шепета та інші.

Метою даної статті є дослідження основних видів шахрайства із використанням банківських платіжних карток та визначення перспективних напрямів протидії їх проявам.

Виклад основного матеріалу. Платіжна картка (payment card) — електронний платіжний засіб у вигляді емітованої в установленому законодавством порядку пластикової чи іншого виду картки, що використовується для ініціювання переказу коштів з рахунку платника або з відповідного рахунку банку з метою оплати вартості товару і послуг, перерахування коштів зі своїх рахунків на рахунки інших осіб, отримання коштів у готівковій формі в касах банків чи через банківські автомати, а також здійснення інших операцій, передбачених відповідним договором [1, с. 83]. З'явившись в середині минулого століття, банківські картки набули поширення більш, як в 160 країнах світу і стали невід'ємним атрибутом цивілізованої людини.

Шахрайські оборудки з банківськими картками та рахунками трапляються доволі часто і стають все більш масовим явищем в Україні.

Нечисті на руку спритники знаходять тисячу способів ошукати людей навіть незважаючи на те, що і банківські установи, і поліція проводять профілактичну роботу, надають інформацію громадянам, попереджають про ризики, ситуація все одно не покращується.

Незважаючи на профілактичні заходи, українці почали частіше потерпати від шахрайства з банківським карткам. Кількість незаконних дій з платіжними картами, за якими банки зазнали збитків, за 2018 рік підвищилася до 105,5 тисяч випадків. Водночас у 2017 році їх кількість була 77,6 тисячі. Традиційно найбільшу кількість шахрайських операцій відбувається у великих містах з населенням більше одного мільйона чоловік. Найбільша кількість незаконних дій з платіжними картами, а саме 55,1 тисячі випадків від загальної кількості, у 2018 році відбувалися в мережі Інтернет. Якщо порівнювати ці дані з 2017 роком, то кількість махінацій з банківськими картками в Інтернеті збільшилася в 1,4 рази [2].

Є досить багато способів шахрайства, які з часом змінюються, удосконалюються, набувають нових форм. Сьогодні шахрайство, вчинене з використанням банківських платіжних карток, характеризується зміною форм і видів, що зумовлене різними причинами; при цьому для сучасних шахраїв характерне використання як старих прийомів, так і нових, раніше невідомих.

До основних видів шахрайств із банківськими платіжними картками можна віднести такі:

Скіммер — невелике пристосування для зчитування інформації з магнітної стрічки, яке вміщається в долоні і може вмістити в себе до 200 номерів карток. Зі скіммера дані перевантажуються на комп'ютер, а з нього за допомогою спеціального декодера — на магнітну стрічку викраденої, знайденої або незаконно виготовленої картки. Інформація, яка міститься на магнітній стрічці, потім витискається на картці і ніякого додаткового обладнання чи витрат ця операція не потребує. Скіммери використовуються, як правило, особами, що приймають картки до оплати — офіціантами, адміністраторами, касирами, які копіюють дані з картки два рази — один для оформлення платежу, другий — на скіммер для злочинців [3, с. 215]. Як варіант, на банкомат прикріплюють мініатюрну відеокамеру, яка знімає руку, що вводить PIN-код, і робить запис у модуль пам'яті або передає його дистанційно на комп'ютер шахрая. Загалом у випадку дистанційної передачі шахрай знаходиться недалеко та приймає відеодані за допомогою ноутбука [6].

Щоб уберегтися від даного виду шахрайства необхідно надавати перевагу банкоматам, які знаходяться на території, що охороняється. Також слід звертати увагу на зовнішній вигляд картридера і клавіатури та при наявності стороннього предмету слід спробувати його забрати, оскільки, як правило, пристрої шахраїв легко зсуваються з місця. Для зняття готівки краще використовувати картку з чіпом, оскільки дані з чіпа складніше підробити, а шахраї не витрачають на це час.

Фішинг (англ. fishing — риболовля). Назва даного виду шахрайств походить від англійського fishing (виловлювання на живця). Існує кілька різновидів цього виду шахрайств. Найпростішим є шахрайство по телефону:

шахрай видає себе за працівника банку, і, посилаючись на збій в комп'ютерній системі через втрату даних, просить клієнта нагадати реквізити його карткового рахунку, особисті ідентифікаційні номери, дівоче прізвище матері, день народження та інше. Найчастіше шахраїв цікавить PIN-код, а також код, який зображено на звороті платіжної пластикової карти (CVV2/CVC2 — використовується при здійсненні покупок в мережі Інтернет). Для здійснення шахрайства також може використовуватися пошта, електронна пошта та інші засоби комунікацій. Досить часто, у даному випадку шахраями використовується інформація про клієнтів банку, отримана від недобросовісних працівників банків, що дозволяє ще більше ввести жертву в оману [5].

За цих умов, основною рекомендацією щодо протидії даному виду шахрайства є суворе дотримання конфіденційності інформації відносно карткового рахунку як з боку працівників банку, так і з боку безпосередньо користувачів пластикових платіжних карток. У разі, коли у користувача виникає підозра щодо порушення конфіденційності зазначеної інформації, йому слід вжити заходів щодо блокування такої картки та її наступного перевипуску.

Траппінг є одним з найпростіших шахрайських способів отримання платіжної картки. Для цього злочинець виготовляє з фотоплівки так звану «ліванську петлю», яку можна непомітно помістити в карточкоприймач банкомату. Далі жертва підходить до банкомату, вставляє свій платіжний засіб у вікно прийому карт, вже «обладнане» цим пристроєм, вводить PIN-код, але картка, навіть коли було знято кошти, не повертається. Злочинець у цій ситуації вдало маніпулює розгубленістю особи та обертає на власну користь ту стресову ситуацію, у якій опиняється жертва. Як правило, поруч у цей час знаходиться сам злочинець або ж його співучасник, який, ніби допомагаючи, використовує різноманітні психологічні прийоми, щоб жертва йому повірила та відійшла від банкомату, наприклад, у найближче відділення банку. У цей час шахрай вилучає з банкомату свій пристрій разом з карткою, після чого викрадає гроші з рахунку. Характеризуючи особу жертви варто зазначити, що часто постраждалими стають туристи або жителі іншої місцевості (наприклад, іншого району). Погане знання мови, думаючи, що це технічний збій, відчуття, що свій банк далеко, часто призводить до того, що жертва сприймає місцевого жителя, який цікавиться ситуацію, що склалася, як рятувальника, чим і користуються шахраї [4].

Якщо ви потрапили в подібну ситуацію, необхідно не відходячи від банкомата уважно оглянути пристрій для видачі грошей, а якщо вони не показуються, відразу зателефонувати до довідкового центру банку.

Ще одним видом шахрайства є дії, що здійснюються із використанням підроблених Інтернет-ресурсів. У даному випадку, для збору даних про платіжні карти шахраями використовуються спеціально створені сайти. Досить часто шахраї намагаються вибрати популярні ресурси, доменні імена яких тільки на одну-дві букви відрізняються від загальновідомих ресурсів, що продають товари або послуги. На таких

Інтернет-ресурсах клієнтам пропонується ввести реквізити платіжної картки для оплати певної послуги, або товару. Але фактично послуга (товар) не надається, а відбувається тільки збір даних про платіжні карти клієнтів для їх подальшого використання.

Для запобігання даному виду шахрайства рекомендується бути більш уважним при здійсненні покупок у мережі Інтернет. Зокрема, слід звертати увагу на адресу сайту, на якому проводяться покупки; використовувати виключно сторінки із захищеним з'єднанням тощо.

Також, дані платіжної картки можуть стати доступні шахраям в разі зараження вашого персонально комп'ютера, телефону або іншого пристрою, з якого ви робите оплату, вірусом. Вірус може потрапити на комп'ютер як за допомогою електронної пошти після спам-розсилки, так і сайту мережі Інтернет. Із зараженого комп'ютера достатньо здійснити хоча б одну легальну покупку в Інтернет (на нормально функціонуючому сайті), і вірус під час проведення платежу збереже всю банківську інформацію і направить її у розпорядження шахраїв.

Основним напрямом протидії даному виду шахрайства є дотримання вимог інформаційної безпеки на персональному комп'ютері, що використовується для транзакцій у мережі Інтернет (наявність антивірусного програмного забезпечення та використання легального програмного забезпечення). Оплату слід проводити тільки на тих веб-сайтах, які також захищені від зовнішніх загроз. Сторінка для оплати повинна мати захищене з'єднання, тобто адреса повинна починатися з <https>. Ніколи не розраховуйтеся карткою на підозрілих сайтах і не вводьте дані карти, якщо сайт обіцяє вам грошовий приз. Це ще один виверт шахраїв. Найкраще завести для інтернет платежів окрему картку і встановити на неї мінімальний ліміт на проведення операцій.

Наведений перелік видів шахрайства із банківськими картками та напрямів їх протидії не є виключним. Разом з тим, дослідження навіть основних напрямів протидії шахрайствам із використанням банківських платіжних карток, свідчить про те, що окремі із показників безпеки інформації можуть бути досягнуті виключно із застосуванням додаткових механізмів технічного захисту інформації, яка зберігається на банківських платіжних картках [8]. Одним із таких механізмів є використання чіп-модулів на банківських платіжних картках. Сучасні науковці зазначають, що саме банківські платіжні картки із чіпами мають найбільший рівень захисту інформації від шахрайських операцій [7, с. 30].

Висновки. Сучасний стан розвитку суспільних відносин у банківській сфері характеризується значним підвищенням активності з боку шахраїв. Наразі можна стверджувати, що злочинці стають більш винахідливими задля отримання вигоди. Таким чином, шахрайство з банківськими картками має значні негативні наслідки для стабільності фінансової системи, оскільки гальмує поширення безготівкової форми оплати, яка є визнаним пріоритетом розвитку світової фінансової системи, а також завдає значної економічної шкоди для різних суб'єктів господарювання. Тому активна боротьба із даним

проявом злочинності — це нагальна вимога часу, що потребує консолідації зусиль банківських установ, правоохоронних органів, громадських організацій та, звичайно, користувачів банківських карток.

До основних способів запобігання вчиненню злочинів пов'язаних із шахрайськими діями в банківській системі слід віднести: розробку нормативної бази з питання забезпечення безпеки банківської системи України; внутрішній контроль можливих загроз з боку служби безпеки банківських установ; запровадження нових, більш досконаліх, технологій у банківську діяльність; запровадження нових, більш захищених форм пластикових карток; врахування позитивного міжнародного досвіду в боротьбі з банківським шахрайством; підвищення обізнаності користувачів банківських карток про ефективні способи захисту власної інформації та правила безпечного використання платіжних карток, електронних платежів і банкоматів; вдосконалення взаємодії між банками, патрульною поліцією, кіберполіцією і слідством при розслідуванні та протидії злочинам з платіжними картками, електронними платежами і з банкоматами; удосконалення кримінального законодавства України в сфері неправомірного використання засобів платежу та приведення його у відповідність до світових стандартів і поширених видів карткових і платіжних злочинів.

Література:

1. Ключко А. М. Шахрайство з використанням банківських платіжних карток / Ключко А. М., Єременко А. О. // Юридичний науковий електронний журнал. — 2016. — № 1. — С.82–86.
2. Матеріали із сайту «Znaj.ua». [Електронний ресурс]. — Режим доступу: <https://znaj.ua/society/220115-v-ukraini-aktivizovalasya-nova-shema-shahrajstva-postrazhdali-tisyachi-vlasnikiv-kartok-yak-vberegitsiya>
3. Осика І. М. Огляд Міжнародного науково-практичного семінару «Протидія економічній злочинності» / Осика І. М. // Право і Безпека. — 2003. — Т. 2, — № 2. — С. 213–219.
4. Олійничук О. І. Правові основи протидії економічній злочинності: навч. посіб. / О. І. Олійничук. — Тернопіль : ФОП Шпак В. Б., 2016. — 242 с.
5. Правовий простір. Шахрайство. Як захиститися та як діяти у разі обману? [Електронний ресурс]. — Режим доступу: <http://legalspace.org/ua/biblioteka/item/9748-shakhraistvo-yak-zakhystytysia-ta-iak-diiaty-u-razi-obmanu>.
6. Скімінг у банкоматах [Електронний ресурс]. — Режим доступу : <http://www.chclub.ru/skimmingatm>.
7. Біломістна І. І. Сучасні тенденції розвитку ринку банківських платіжних карток в Україні / І. І. Біломістна // Економічні науки. — 2012. — № 9. — С. 26–36.
8. Шепета О.В. Перспективні напрями протидії шахрайствам із використанням банківських платіжних карток. [Електронний ресурс]. — Режим доступу: <http://goal-int.org/perspektivni-napryami-protidii-shahrajstvam-iz-vikoristannyam-bankivskix-platizhnix-kartok>

References:

1. Klochko A.M., Yeremenko A.O. Shakhrajstvo z vykorystanniam bankivs'kykh platizhnykh kartok. Yurydychnyj naukovyj elektronnyj zhurnal. — 2016. — №1. S.82–86.
2. Materialy iz sajta «Znaj.ua». [Elektronnyj resurs]. — Rezhym dostupu: <https://znaj.ua/society/220115-v-ukraini-aktivizuvalasya-nova-shema-shahrajstva-postrazhdali-tisyachi-vlasnikiv-kartok-yak-vberegitsya>
3. Osyka I. M. Ohliad Mizhnarodnoho naukovo-praktychnoho seminaru «Protydiia ekonomichnij zlochynnosti» // Pravo i Bezpeka. — 2003. — Т. 2, № 2. — S. 213-219.
4. Olijnychuk O. I. Pravovi osnovy protydii ekonomichnij zlochynnosti: navch. posib. / O. I. Olijnychuk. — Ternopil' : FOP Shpak V. B., 2016. — 242 s.
5. Pravovyj prostir. Shakhrajstvo. Yak zakhystytysia ta iak diiaty u razi obmanu? [Elektronnyj resurs]. — Rezhym dostupu: <http://legalspace.org/ua/biblioteka/item/9748-shakhraistvo-yak-zakhystytysia-ta-iak-diiaty-u-razi-obmanu>
6. Skiminh u bankomatakh [Elektronnyj resurs]. — Rezhym dostupu : <http://www.chclub.ru/skimmingatm>.
7. Bilomistna I. I. Suchasni tendentsii rozvytku rynku bankivs'kykh platizhnykh kartok v Ukraini / I.I. Bilomistna // Ekonomichni nauky. — 2012. — № 9. — S. 26–36.
8. Shepeta O. V. Perspektyvni napriamy protydii shakhrajstvam iz vykorystanniam bankivs'kykh platizhnykh kartok. [Elektronnyj resurs]. — Rezhym dostupu: <http://goal-int.org/perspektivni-napryami-protidii-shaxrajstvam-iz-vikoristannyam-bankivskix-platizhnix-kartok>