УДК 343.72:336.717
DOI https://doi.org/10.32782/2524-0374/2022-11/90

ШАХРАЙСТВО У СФЕРІ ОБІГУ БАНКІВСЬКИХ ПЛАТІЖНИХ КАРТОК: КРИМІНАЛЬНО-ПРАВОВИЙ АСПЕКТ

FRAUD IN THE FIELD OF BANKING PAYMENTS CARD: CRIMINAL-LEGAL ASPECT

Огієвич А.О., студентка ІІІ курсу факультету прокуратури
Національний юридичний університет імені Ярослава Мудрого

Романова А.Є., студентка ІІІ курсу факультету прокуратури
Національний юридичний університет імені Ярослава Мудрого

На сьогодні розрахунки у безготівковій формі отримали значну поширеність, але через таке зростання збільшилася і кількість шахрайських спроб використання даних про карткових користувачів для незаконного збагачення. За даними Нацбанку України, лише за минулий рік в Україні сталося майже 72 тисячі випадків незаконних дій із платіжними картами, 58% із яких сталися в Інтернеті. Уже в першому півріччі минулого року банки повідомили про фіксацію 47,5 тис. випадків шахрайства з картками на загальну суму 86,4 млн грн. Банківські установи також зазнають значної шкоди від таких дій, адже несуть певну відповідальність при здійсненні операцій за допомогою платіжної картки, якщо йдеться про операції, які відбуваються за твердженням користувачів, не були ними погоджені, про що вони повідомили банк-емітент. Також, у зв'язку з введенням воєнного стану в Україні з 24 лютого 2022 року, почали з'являтися нові види шахрайства які потребують детального аналізу.

Тому дослідження питань шахрайства з банківськими картками та протидії цьому явищу є надзвичайно актуальним в умовах розвитку інформаційних технологій в банківському секторі та поширення їхнього використання.

Метою цієї статті є висвітлення нових аспектів шахрайства, способи його вчинення та відповідальність за такі дії під час воєнного стану.

Різні аспекти дослідження новітніх шахрайських дій з використанням сучасних програмно-технічних засобів, зокрема в банківському секторі, окреслено у багатьох працях останніх років. Науковці: Т. В. Романенко, С. В. Шапочка висвітлили питання боротьби з шахрайством, яке вчиняється з використанням можливостей мережі Інтернет [6]. С. В. Поперешняк розглянув основні ризики, що супроводжують карткові технології та методи захисту учасників карткових операцій [7]. С. В. Самойлов описав типові слідчі ситуації початкового етапу розслідування шахрайств, що вчиняються з використанням мережі Інтернет, відповідні їм слідчі версії та алгоритми їх перевірки [8]. Однак, обстановка, яка наразі наявна в Україні через військову агресію з боку Російської Федерації спричинили появу нових різноманітних видів шахрайства, які потребують дослідження.

Ключові слова: шахрайство, фішинг, банківські картки, кардинг, Інтернет-шахрайство, схеми шахраїв.

Today, cashless payments have gained great popularity, but due to this growth, the number of fraudulent attempts to use data on card users for illegal enrichment has also increased. According to the National Bank, almost 72,000 cases of illegal actions with payment cards occurred in Ukraine last year alone, 58% of which occurred on the Internet. Already in the first half of last year, banks reported the recording of 47,500 cases of card fraud for a total amount of UAH 86.4 million. Banking institutions also suffer significant damage from such actions, because they bear a certain responsibility when carrying out operations with the help of a payment card, if it is about operations that take place according to the users, were not agreed by them, about which they informed the issuing bank. Also, in connection with the introduction of martial law in Ukraine from February 24, 2022 by Decree of the President of Ukraine No. 64/2022, new types of fraud began to appear that require detailed analysis.

Therefore, the study of the issues of fraud with bank cards and countering this phenomenon is extremely relevant in the conditions of the development of information technologies in the banking sector and the spread of their use.

The purpose of this article is to highlight new aspects of fraud, ways of committing it and responsibility for such actions during martial law.

Various aspects of the research of the latest fraudulent actions using modern software and technical means, in particular in the banking sector, have been outlined in many works of recent years. Scientists: T. V. Romanenko, S. V. Shapochka highlighted the issue of combating fraud, which is committed using the capabilities of the Internet [6]. C. V. Popereshniak considered the main risks accompanying card technologies and methods of protecting participants in card operations [7]. S. V. Samoilov described typical investigative situations of the initial stage of the investigation of fraud committed using the Internet, corresponding investigative versions and their verification algorithms [8]. However, the circumstances that have currently occurred in Ukraine due to military aggression by the Russian Federation have caused the emergence of new and diverse types of fraud that require research.

Key words: fraud, phishing, bank cards, carding, Internet fraud, fraudsters' schemes.

За останні роки в Україні Інтернет-шахрайство з використанням банківських платіжних карток набуло досить значного поширення. Суспільна небезпечність таких кримінальних правопорушень полягає в тому, що, поряд із посяганням на власність громадян, їхні грошові кошти, які перебувають на банківських рахунках, цей злочин спричиняє шкоду злагодженому функціонуванню банківської системи, цим самим становлячи суттєву небезпеку для суспільства й держави.

Взагалі шахрайство є корисливим злочином проти власності, що передбачено ст. 190 Кримінального кодексу України, і полягає у заволодінні чужим майном або придбанні права на майно шляхом обману чи зловживання довірою [9]. Предметом шахрайства з банківськими картками будуть грошові кошти, які знаходяться у громадян на банківських рахунках. Щодо об'єктивної сторони такого злочину, то він полягає у заволодінні коштів громадян, які мають рахунки в банках, шляхом обману або зловживання довірою.

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

– фішинг (отримання персональних даних власника картки), який має підвиди: смішинг (фішинг саме через SMS-повідомлення), вішинг (фішинг із використанням телефону та схожих пристроїв);

– кардинг (коли реквізити банківських карток шахраї беруть із різних джерел, зокрема зі зламаних серверів, персональних комп'ютерів, через програми віддаленого доступу, через віруси-«трояни», з бухгалтерських документів, сканованих авіаційних квитків тощо), який має підвиди: скимінг (копіювання (зчитування) персональних даних з оригінальної карти на фальшиву), шимінг (поміщення у банкомат шимера – електронного пристрою, який дозволяє отримати злочинцю інформацію про банківську картку клієнта);

– шахрайство з банківськими картками в Інтернеті, яке має підвиди: шахрайські дії у соціальних мережах, фармінг (хакерські дії з направлення на хибну IP-адресу);

скамінг (отримання від власника картки певних коштів з обіцянкою повернути більше);

– шахрайство з банківськими картками у сервісних торгівельних мережах [1].

Звичайно, що це не єдина класифікація видів шахрайства з банківськими платіжними картками, наявні також інші, проте, на нашу думку, вона є основною і часто застосовується на практиці. Усім відомі такі види шахрайства з банківськими картками як «нігерійські листи», які не так давно запроваджені шахраями, та наклейка на шатер – проріз, через який відбувається видача готівки, – пристрою, який блокує видачу купюр.

Також проаналізувавши судово-слідчу практику, ми виділили найхарактерніші способи вчинення злочинів у сфері банківських платіжних карток:

заволодіння коштами шляхом здійснення незаконних операцій з використанням електронно-обчислювальної техніки з метою підроблення банківської платіжної картки;

– підроблення банківської платіжної картки та повторне використання електронно-обчислювальної техніки;

– підроблення банківського рахунку та комплексного надання послуг;

– використання повністю підроблених банківських платіжних карток;

– використання «білого пластику»;

– оплата товарів через комп'ютерну мережу чужими банківськими картками;

– використання кредитної картки на чуже ім'я, отриманої вдруге шахраєм по паспорту власника картки;

– розкрадання коштів працівниками сфери обслуговування шляхом несанкціонованого списування їх з кредитної картки клієнта;

– незаконне збагачення шляхом заволодіння чужим майном, в порушення встановленого порядку виготовлення, використання та обігу платіжних карток;

– спосіб копіювання ПІН-коду шляхом накладної клавіатури або записом мініатюрною відеокамерою. [1]

Отже, способи вчинення кримінального правопорушення з використання банківських платіжних карток можна диференціювати на три основні групи: 1) способи незаконного доступу до банківських рахунків, пов'язані з використанням розрахунків платіжними дорученнями; 2) способи вчинення злочинів, пов'язаних із незаконним доступом до банківських рахунків, пов'язані з використанням операцій у сфері обігу банківських платіжних карток; 3) способи вчинення злочинів, пов'язані з використанням інших засобів доступу до банківських рахунків. [2]

Наше сьогодення, яке пов'язане зі скрутним фінансово-економічним становищем на території України, на наш погляд, створює достатньо умов для того, щоб посягання на банківську систему займали не другорядне значення частини кримінально-правових норм, а були сформовані в окремий розділ у Кримінальному кодексі України «Кримінальні правопорушення у сфері банківської діяльності». Також варто наголосити, що різні автори по різному визначають кваліфікацію шахрайства з банківськими картками.

На думку О. О. Дудорова , суспільно небезпечні посягання на власність, які вчиняють з використанням платіжних карток або їх реквізитів і які врешті-решт призводять до несанкціонованого законним держателем картки переказу грошових коштів з його рахунка, є підстави кваліфікувати не як крадіжку, а за ст. 190 КК України як шахрайство. [3]

А інші вчені такі як А. М. Черняк, А. Ю. Прозоров, Д. В. Пашнєв, А. А. Васильєв, вказують на те , що окремий вид шахрайства з банківським картками кваліфікується по різному і потребує детально аналізу в кожному окремому випадку. Так, дискусійним залишається питання правової кваліфікації такого злочину, як фармінг. Об'єктивна сторона його полягає в тому, що процедуру отримання зловмисниками доступу до конфіденційної інформації, пов'язаної з банківським рахунком потерпілого, усупереч його волі в прихований спосіб через використання спеціального програмного забезпечення та здійснення незаконних фінансових операцій без його відома.

Таким чином, незаконне вилучення грошових коштів зловмисниками з банківського рахунку потерпілого шляхом використання фармінгу в деяких випадках може бути кваліфіковано як крадіжка (ст. 185 КК України).

Деякі різновиди інтернет-шахрайства з банківськими платіжними картками мають також ознаки складу злочину, передбаченого ст. 200 КК України, де кримінальну відповідальність за підроблення документів на переказ, платіжних карток чи інших засобів доступу до банківських рахунків, електронних грошей, а так само придбання, зберігання, перевезення, пересилання з метою збуту підроблених документів на переказ, платіжних карток або їх використання чи збут, а також неправомірний випуск або використання електронних грошей. Із цього слідує, що безпосереднім об'єктом цього злочину є встановлений порядок проведення грошових розрахунків, виготовлення та обігу платіжних документів й інших засобів доступу до банківських рахунків, майнові права та інтереси юридичних і фізичних осіб – учасників розрахункових відносин, зокрема емітентів та держателів платіжних карток.

Але особливу увагу ми хочемо приділити новим видам шахрайства, які виникли в умовах повномасштабної війни, бо шахраї не змінили своєї тактики, а навпаки, знаючи душевний стан більшості населення, у тому числі тих, хто був змушений залишити свої домівки та орендувати житло в інших містах і взагалі втратили джерело доходу, злочинці почали впроваджувати нові схеми шахрайства банківських карток, в яких простежується ряд спільних рис.

У своїх діях шахраї маніпулюють емоціями своїх жертв, акцентуючи увагу на почуттях провини, жалю та страху. Текстові повідомлення шахраїв можуть містити багато російських слів, орфографічні та інші помилки. Шахраї намагаються скористатися скрутним становищем потенційних жертв. Вони можуть дзвонити та вимагати гроші за те, що вони володіють інформацією про місце перебування родичів, яких останні шукають.

До однієї з найпоширеніших схем в умовах сьогодення відносять **«посередницькі» послуги від шахраїв».** Шахраї нібито пропонують посередницькі послуги для отримання гарантованої винагороди з фондів гарантування вкладів фізичних осіб. За такі послуги просять «комісію».

Тут слід бути обережним та не співпрацювати з шахраями, бо гарантовані виплати-винагороди здійснюються виключно через довірений банк Фонду, який підключений до автоматизованої системи виплат.

Дане діяння повністю підпадає під ознаки шахрайства, а саме статтю 190 КК , бо завдяки зловживанню довірою особа отримує кошти від особи, яка думає, що отримує допомогу, а отже має місце цей склад злочину. [5]

Також має місце така схема шахрайства як **SMS-повідомлення про надходження платежу.** Шахраї надсилають SMS-повідомлення клієнтам банків, нібито вони отримали платежі на їхні рахунки. Такі SMS-повідомлення містять фішингові посилання. За ними шахраї можуть отримати дані банківської картки та особисті дані. Окрім SMS, шахраї можуть розсилати шкідливі посилання в месенджерах та електронних листах.

Щодо кваліфікації, то таке діями ми відносимо до статті 185 КК, оскільки обман або зловживання довірою було використано задля доступу до майна у таємний спосіб, що характерне для об'єктивної сторони крадіжки. Також можлива сукупність, оскільки особа також створила посилання для вчинення крадіжки, відповідальність за що передбачено статтею 361 КК , а саме створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут. [5]

Наступною схемою є **фейкові оголошення про оренду житла**. Шахраї розміщують неправдиві оголошення про те, що готові здати квартири переселенцям у безпечних районах, а потім вимагають передоплату на картку та відключають відповідні номери після отримання коштів.

Дану схему , на нашу думку, можна кваліфікувати за статтею 190 КК України, бо наявний склад злочину, а саме об'єктивна сторона шахрайства, яка характеризується тим, що потерпілий добровільно, унаслідок обману чи використання винним його довіри, передає грошові кошти злочинцю. [5].

«Евакуаційний транспорт громадян» також є одним з найпоширеніших схем злочинців. Шахраї можуть запропонувати транспортування з гарячих точок до безпечних місць. Шахраї вимагають сплати на картку наперед, але не виконують своїх зобов'язань і просто зникають.

Кваліфікація даної схеми також можлива за статтею 190 КК, оскільки наявні ознаки складу даного правопорушення.

Зараз доволі часто шахраї **зламують сторінки в соцмережах**, наприклад, Facebook. Самозванець створює публікацію на сторінці її власника і від його імені просить фінансову допомогу для придбання амуніції у зв'язку з від'їздом на фронт. Також створюють фейкові оголошення для збору коштів на лікування дітей, які нібито постраждали від військової агресії. Бувають випадки, коли шахраї знаходять в Інтернеті фотографії своїх жертв і збирають гроші «на допомогу» для неї.

У даній схемі має місце, кваліфікація за сукупністю ч. 3 статті 190 КК , оскільки особа шляхом використання обману підписників власника сторінки присвоює собі кошті, а також статті 361 КК України, бо особа несанкціоновано втручається в роботу Інтернет-сторінки .

Схожою схемою на попередні є **«неправдива реклама продажу військової амуніції».** Шахраї можуть розміщувати в Інтернеті оголошення про продаж бронежилетів та інших військових речей. Після отримання переказу шахрай зникає. Крім того, деякі продавці можуть бути шахраями, наприклад, продаючи несправну броню, яка не захищає солдатів від куль. [4]

У даному випадку можливі різні варіанти кваліфікації, бо у першу варіанті, де просто зникає продавец, наявні ознаки шахрайства, відповідно до статті 190 КК, а у другому випадку, обман може призвести до різних наслідків, а саме смерті або поранення військового, через не справжню броню, тому таке діяння повинне кваліфікуватися за сукупністю злочинів, дивлячись на наслідки, які настануть.

Отже, уведення в оману є тією визначальною обставиною, яка дає змогу відмежувати шахрайство від інших корисливих злочинів проти власності. Суспільно небезпечні посягання на власність, які вчиняють з ст. 185 КК України використанням платіжних карток або реквізитів і які, зрештою, призводять до несанкціонованого переказу коштів з рахунків, є підставою кваліфікувати не як крадіжку, а за ст. 190 КК України як шахрайство. Також цей вид шахрайства може бути додатково кваліфікований за статтями 361–361-1 Кримінального кодексу України. Зокрема, додаткової кваліфікації за ст. 361 КК вимагає шахрайство, вчинене шляхом ініціювання незаконної транзакції в платіжній системі від імені потерпілої особи, у тих випадках, коли необхідні для транзакції реквізити були отримані за допомогою несанкціонованого втручання в роботу комп'ютерної мережі (наприклад, шляхом «зламу» електронної поштової скриньки) [2]. У такий спосіб, доступ до банківських рахунків, який отриманий шахраями у незаконний спосіб, може бути пов'язаним між собою з кримінально-караними діяннями проти власності (ст. 185, 190, 191 КК України), у сфері господарської діяльності (ст. 200, 205, 209, 231 КК України), використання електронно-обчислюваних систем комп'ютерних мереж (ст. 361, 361-1, 362 КК України), службової діяльності.

На жаль, вітчизняна правоохоронна система в Україні поки не готова до ефективної боротьби зі злочинами, пов'язаними з банківськими платіжними картками, у силу низки причин. Тому існує необхідність вжиття першочергових заходів, спрямованих на протидію та боротьбу з такими шкідливими проявами. Зокрема, важливим є питання діяльності відповідних підрозділів, які здійснюватимуть розслідування виключно цієї категорії злочинів. Зараз це входить до компетенції такого структурного підрозділу як Департамент кіберполіції Національної поліції України.

Цікавою є Постанова апеляційного суду міста Києва від 28.12.2017 року у справі № 761/42973/17 з якої відомо, що Службою безпеки України здійснюється досудове розслідування в кримінальному провадженні № 22017000000000363 від 10 жовтня 2017 року за ознаками кримінальних правопорушень, передбачених ч. 4 ст. 190, ч. 2 ст. 200, ч. 3 ст. 209 КК України. За версією слідства, особа створила злочинну схему заволодіння коштами з банківських карток третіх осіб. Зокрема, він купував в Інтернеті дані платіжних карток, необхідні для створення дублікатів та після чого мав можливість їх використовувати, але з деякими обмеженнями.

За кілька років діяльності організованої злочинної групи, було придбано товарів через Інтернет на суму понад 3 мільйони доларів США з використанням даних платіжних карток третіх осіб. Організатору даної схеми навіть було повідомлено про підозру у вчиненні злочинів, передбачених ч. 4 ст. 190, ч. 2 ст. 200, ч. 3 ст. 209 КК України (шахрайство в особливо великих розмірах, підробка платіжних карток, вчинена повторно та за попередньою змовою групою осіб, а також легалізація майна, одержаного злочинним шляхом). Проте вирок у даному провадженні в Єдиному реєстрі судових рішень відсутній, що в черговий раз демонструє недостатню ефективність притягнення до відповідальності винних осіб [10].

Отже, на сьогоднішній день в Україні розвинена система шахрайства з банківськими картками, яка дуже загострилась з початком активних бойових дій. Нові схеми з'являються на ґрунті потреб населення в ці не прості для країни часи. На жаль, повернути такі кошти практично неможливо. У даній статті ми висвітлили нові схеми шахраїв, які зловживаючи довірою, шоковим станом багатьох громадян та отримають цим шляхом матеріальну вигоду. На прикладах нових схем ми розкрили основні методи, якими користуються правопорушники. Хоча банківська система разом з Національною поліцією, протягом багатьох років проводила різноманітні дії, спрямовані на запобігання таким злочинам, навчання людей протистояти таким діям, але поради щодо захисту від шахраїв миттєво забуваються людьми у стресових ситуаціях. Тому, заради належного регулювання повинна бути створена всебічна протидія таким видам шахрайства .

Також на наш погляд, сьогоднішня ситуація створює достатньо умов для того, щоб посягання на банківську систему займали не другорядне значення частини кримінально-правових норм, а були сформовані в окремий розділ у Кримінальному кодексі України «Кримінальні правопорушення у сфері банківської діяльності», що полегшить притягнення таких осіб до відповідальності та передбачить різноманітні види кваліфікації таких діянь.

ЛІТЕРАТУРА

1. Сьоміна Н. А. Банківська платіжна картка як знаряддя шахрайських дій: поняття та основні способи. *Актуальні проблеми вдосконалення чинного законодавства України* : збірник наукових статей. 2016. Вип. 40. С. 149-156. URL: http://nbuv.gov.ua/UJRN/apvchzu_2016_40_18 (дата звернення: 12.11.2022).

2. Кришевич О. В. Способи шахрайств в банківській сфері: кримінально-правовий аспект. *Юридичний вісник*. 2012. № 2(23). С. 112-116. URL: http://nbuv.gov.ua/UJRN/Npnau_2012_2_25 (дата звернення: 12.11.2022).

3. Черняк А. М., Прозоров А. Ю. Аспекти запобігання правопорушенням у сфері використання банківських платіжних карток під час проведення безконтактних й інтернет-платежів та їх кваліфікація. *Науковий вісник Національної академії внутрішніх справ*. 2019. № 4 С. 8-14.

4. Про нові види шахрайства у банківській системі. *Фінансовий клуб*: веб-сайт. URL: http://www.finclub.net (дата звернення: 14.11.2022).

5. Як уберегтися від шахрайства? *Мотор банк* : веб-сайт. URL: https://motor-bank.ua/ (дата звернення: 14.11.2022).

6. Романенко Т. В. Особливості слідової картини шахрайств, що вчиняються в мережі Інтернет. *Молодий вчений*. 2016. № 1(2). С. 51–54.

7. Поперешняк С. В. Ризики та алгоритми захисту сучасних банківських карткових технологій. *Вісник соціально-економічних досліджень*. 2013. Вип. 2(2). С. 60–67.

8. Самойлов С. В. Типові слідчі ситуації початкового етапу розслідування шахрайств, що вчиняються з використанням мережі «Інтернет», відповідні їм слідчі версії та алгоритми їх перевірки. *Проблеми правознавства та правоохоронної діяльності.* 2014. № 4. С. 25–31.

9. Кримінальний кодекс України : Кодекс України від 05.04.2001 р. № 2341-III : станом на 6 листоп. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 14.11.2022).

10. Система притягнення до відповідальності за шахрайство з банківськими картками не є ефективною в Україні. *Правовий Альянс*:веб-сайт.URL:https://www.legalalliance.com.ua/publikacii/sistema-pritagnenna-do-vidpovidalnosti-za-sahrajstvo-z-bankivskimi-kartkami-ne-e-efektivnou-v-ukraini/ (дата звернення: 17.11.2022).