Пивоваров В.В.,
кандидат юридичних наук,
доцент кафедри кримінології та кримінально-виконавчого права
Національного юридичного університету імені Ярослава Мудрого

Терещенко К.В.,
студентка, бакалавр права
Інституту підготовки кадрів для органів прокуратури
Національного юридичного університету імені Ярослава Мудрого

ШАХРАЙСТВО ІЗ БАНКІВСЬКИМИ КАРТКАМИ: ОКРЕМІ ПИТАННЯ ВІКТИМОЛОГІЧНОЇ ПРОФІЛАКТИКИ

Анотація: У статті досліджується шахрайство із банківськими картками, способи його вчинення, особа жертви від цього злочину та окремі питання віктимологічної профілактики.

Аннотация: В статье исследуется мошенничество с банковскими карточками, способы его совершения, личность жертвы от указанного преступления и отдельные вопросы виктимологической профилактики.

Summary: The article research fraud with bank cards, ways of its committing, personality of a victim from this type of crime and separate questions of victimological prevention.

Постановка проблеми. На сьогоднішній день новітні технології дозволяють злочинцям використовувати найрізноманітніші сучасні способи порушення закону, які, в той же час, мають латентний характер. Дуже поширеним видом злочину проти власності стає шахрайство з банківськими картками. Як вірно зазначає Пивоваров В. В., латентна злочинність в банківській сфері – це яскравий і наглядний прояв корпоративної злочинності, що функціонує в сфері банківської діяльності [1]. Шахрайство, що вчиняється з використанням комп'ютерних мереж, банкоматів, платіжних і банківських карток, є порівняно новим видом злочину, котрий характеризується високим рівнем латентності, а тому потребує самостійних кримінологічних досліджень.

Аналіз останніх досліджень. Із розвитком новітніх технологій, комп'ютеризацією, запровадженням та стрімким поширенням платіжних інструментів, до яких відносяться і банківські картки, зростає та урізноманітнюється відповідно кількість вчинюваних злочинів у сфері банківських відносин. Головним при цьому є те, що посягаючи таким чином на власність певних осіб, злочинці наносять збитки і інформаційній та економічній безпеці держави в цілому. Через свою очевидну актуальність ця тема розглядалась багатьма науковцями, серед яких: О. І. Барановський, І.І. Попович, О.А. Самойленко, С.В. Шапочка, В.Г. Хахановський та інші.

Однак зазначена тема розглядалася головним чином з точку зору наук кримінального права та криміналістики, оминаючи дуже важливі кримінологічні питання, що неодмінно мають бути розглянуті задля повної характеристики такого виду шахрайства, як шахрайство

з банківськими картками. Аналіз саме кримінологічних питань, зокрема, особи жертви та її віктимної поведінки, в свою чергу дозволить зробити важливі кроки для запобігання вказаному виду злочинів та зменшення кількості потерпілих.

Метою даної статті є вирішення питань віктимологічної профілактики стосовно шахрайства з банківськими картками.

Виклад основного матеріалу. Сфера банківських відносин є однією з найважливіших складових, що забезпечують сталий розвиток держави. Без її належного функціонування неможливо говорити про економічну безпеку країни.

Наразі розвиток технологій дозволив використовувати найрізноманітніші засоби розрахунків, платіжні інструменти, які вводяться у фінансовий обіг та вже є загальноприйнятними. Майже кожна особа хоча б раз у житті користувалася банкоматами для отримання готівки або переказу коштів. Використання банківських платіжних карток, з одного боку, може полегшити розрахунки, спростити їх та зекономити час, дати змогу особі отримати свої гроші майже будь – де та коли завгодно. Однак разом з тим це породжує і нові ризики, адже шахраї стають також більш винахідливими. Сучасні технології не лише допомагають у боротьбі проти злочинності, але, на жаль, також сприяють самим злочинцям у реалізації їх намірів.

Відповідно до Закону «Про платіжні системи та переказ коштів в Україні» [2], платіжна картка – це електронний платіжний засіб у вигляді емітованої в установленому законодавством порядку пластикової чи іншого виду картки, що використовується для ініціювання переказу коштів з рахунка платника або з відповідного рахунка банку з метою оплати вартості товарів і послуг, перерахування коштів зі своїх рахунків на рахунки інших осіб, отримання коштів у готівковій формі в касах банків через банківські автомати, а також здійснення інших операцій, передбачених відповідним договором.

Наразі вже відомо багато видів шахрайства з банківськими картками та банкоматами: «скімінг», «траппінг», «фантом», «шаттер», «шиммінг», а також «трешинг», «фармінг», «фітинг». Хоча обрання злочинцем певного способу не впливає загалом на кваліфікацію його діяння з точки зору кримінального права, однак свідчить про те, що злочинці стають більш винахідливими, залучаючи для незаконної діяльності сучасні технології. Крім цього, поведінка потерпілого та у зв'язку з цим, комплекс дій злочинця у різних ситуаціях є неоднаковими. Для з'ясування особливостей поведінки жертви доцільним є дослідження вищезазначених способів шахрайства.

Один зі способів украсти гроші з картки – скімінг. Шахраї встановлюють на банкомати спеціальні пристрої – скімери, які зчитують номер та пін-код. Далі картка дублюється і гроші міняють власника за лічені хвилини. Як варіант на банкомат прикріплюють мініатюрну відеокамеру, яка знімає руку, що вводить пін-код і робить запис у модуль памяті або передає його дистанційно на комп'ютер шахрая. Загалом, у випадку дистанційної передачі шахрай знаходиться неда-леко та приймає відеодані за допомогою ноутбука. Скіммінг ж в чистому вигляді не вимагає безпосереднього знаходження шахрая біля банкомату і своїх жертв.

«Шиммінг» є однією з останніх вигадок викрадачів, одним із способів незаконного зняття грошей за допомогою використання тонкої плівочки, схожої на скотч. Така плівка наклеюється на клаві-

атуру, а потім із неї зчитується необхідна інформація. Незвичайна клавіатура банкомата не викликає підозри, що значно полегшує завдання злочинцям [3].

Траппінг є одним з найпростіших (з точки зору операційних витрат) способів роздобути платіжну картку з PIN-кодом. 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 прийому, щоб жертва йому повірила та відійшла від банкомату, наприклад, у найближче відділення банку. У цей час шахрай вилучає з банкомату свій пристрій разом 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, відчуття, що свій банк далеко, часто призводить до того, що жертва сприймає місцевого жителя, який цікавиться ситуацією, що склалася, як рятівника, чим і користуються шахраї.

Нерідко трапляються навіть випадки повної підміни банкомату. На вид звичайний банкомат є муляжем, обладнаним спеціальними пристроями зчитування інформації. При цьому на ньому будуть відображатись запити, відповідні поля вводу даних, однак на завершальній стадії гроші не будуть видані ніби через їх відсутність. Таким чином злочинець отримує у цифровій формі всю необхідну інформацію для подальших махінацій. Такий спосіб називається «фантом».

Ще одним способом шахрайства з банкоматами є шаттер, що полягає у блокуванні видачі самої готівки. Для цього на шаттер (проріз, через яку відбувається видача грошей) наклеюється сторонній пристрій, блокуючий видачу купюр банкоматом власнику картки. Відбувається це за рахунок розміщення липкої стрічки на внутрішній частині пристрою, до якої пристають купюри. Шахрай, що з'явиться одразу, як піде жертва, отримає таким чином зняту суму.

Наряду із шахрайством з банкоматами, існує і шахрайство з платіжними картками. Так, «фармінг» полягає у тому, що під час знаходження на певному сайті, на комп'ютер жертви потрапляє вірус. Коли особа заходить на сайти інтернет – банкінгу, тощо, вірус, що проникнув у систему, переадресовує її до фіктивного сайту, який зовнішньо є якщо не ідентичним, то максимально подібним до справжнього, а потім введена клієнтом інформація фіксується злочинцем для подальших шахрайських дій.

«Фішинг» є одним з найпоширеніших способів шахрайства з платіжними картками, спрямований на одержання від жертви конфіденційної інформації про реквізити картки. На сьогодні виділяють три види «фішингу» – поштовий, онлайновий та комбінований [4]. Однак, на меті злочинця у будь – якому разі є отримання реквізитів банківської картки.

Особливістю досліджуваного виду шахрайства є безпосередня участь особи потерпілого у вчиненні злочинцем правопорушення. Таким чином, наявна «посередницька» діяльність жертви. Ви-

вчаючи типові різновиди її поведінки, особистісні характеристики, можна суттєво зменшити потенційні ризики щодо широких верств населення.

Фатальний збіг обставин, за якими жертва опинилася не в тому місці, не в той час, для таких злочинів не характерний. Віктимна ситуація виникає як результат опосередкованого зв'язку між злочинцем і жертвою, але навіть при несприятливій ситуації у особи є можливість запобігти злочину.

Щодо шахрайства детермінантами індивідуальної віктимності можуть виступати найрізноманітніші властивості особи, наприклад, її низький інтелект, погана адаптованість, недостатня обізнаність, психологія жадібності тощо. Часто жертвами від даного виду злочину стають особи похилого віку через недостатню поінформованість у сучасних технологіях, зокрема, у сфері банківської діяльності, знижену увагу. Часто жертвами шахрайства з банкоматами (зокрема, шляхом «траппінгу» та способом «фантом»), стають особи, що не проживають постійно на відповідній місцевості, туристи. Недостатня обізнаність у комплексі зі стресовою ситуацією, створеною шахраєм, сприяє віктимізації таких осіб та привертає до них підвищену увагу злочинців. До найбільш часто застосованих методів кримінального маніпулювання при шахрайстві належать: використання психологічного автоматизму, маніпуляції змістом і формою наданої інформації, зміна темпів її надання, експлуатація фонових станів, використання групового впливу на обличчя. Застосування сучасних психотехнологій спрямованого впливу робить вразливим у шахрайських зазіханнях значне коло осіб, які не мають характерних психологічних і соціально – демографічних особливостей, потерпілих від шахрайства. Цей процесс являє собою систему взаємопов'язаних і організаційно підготовлених методів і прийомів впливу на жертву [5].

У сфері шахрайства з банківськими картками визначальну роль відіграє поведінка жертви. Як зазначають науковці, основними причинами скоєння злочину є неуважність самої жертви, відсутність в неї достатньої критичності мислення, власна необачність та схильність до ризику. Так, на думку К. Л. Попова, часто ризик стає для людини останнім аргументом на користь участі у ситуаціях невизначеності чи непевності, які передбачають отримання суттєвих благ, досягнення значних переваг, але разом з тим є потенційно небезпечними з огляду на можливість неприємних наслідків на виході [6].

Критичність поведінки жертв шахрайства визначає низка чинників: соціальний досвід людини, її поінформованість у різних сферах життя: економічній, кримінологічній, юридичній, психологічній. При цьому у поінформованості науковці пропонують виділяти: загальну соціальну (тобто набутий життєвий досвід особи), правову (одержані правові знання) та кримінологічну (віктимологічну).

З огляду на все вищезазначене, необхідно поєднати досвід із попередження віктимологічної поведінки, що послідовно знаходить своє відображення у працях відомих кримінологів із досягненнями наукового прогресу, що, безперечно, дозволить досягти більш вагомого результату.

На даний момент вже здійснено важливі кроки у цьому напрямку. Так, за ініціативою Незалежної асоціації банків України створено спеціальний сайт [7], на якому зосереджена інформація про розповсюджені схеми та поради учасни-

кам банківських відносин щодо того, як не стати жертвою злочину.

Однак, навряд це є достатнім для того, щоб запобігти віктимологічної поведінки осіб. Оскільки вчинення цього злочину насамперед залежить саме від дій жертви, необхідно, перш за все, активно і різноманітно інформувати осіб, що користуються послугами банків, про всі можливі ризики та належні заходи безпеки. Також доцільним було б розміщення у банківських установах відповідних інформаційних стендів, які б роз'яснювали, як правильно використовувати банківські картки, як не стати жертвою шахрайства, розміщувати цю інформацію на сайтах банків, запровадити інструктаж клієнтів працівниками банку.

Оскільки сама жертва є необхідним «посередником» вчинення шахрайства з банківськими картками, то, перш за все, необхідно роз'яснювати особам належні заходи запобігання цьому виду злочинів: нікому не повідомляти реквізити банківських карток, коди, уважно оглядати банкомати, якщо є сумнів у їх справжності, не надавати своїх персональних даних на сумнівних сайтах, не відповідати на підозріли листи тощо.

Варто зазначити, що запобігання злочинності шляхом усунення віктимної поведінки осіб, які потерпають від банківського шахрайства, потребує комплексного підходу: покращення загального рівня життя, соціального забезпечення, законодавчого врегулювання, врахування досвіду інших країн в галузі віктимологічної профілактики.

Висновок. Наразі можна упевнено стверджувати, що злочинці стають більш винахідливими задля отримання вигоди. Комп'ютеризація та розвиток інформаційних технологій, мережі Інтернет на сьогоднішній день стають невід'ємною складовою життя людини. Розширюються можливості розрахунків, вводяться в обіг різноманітні платіжні інструменти. Серед них одним з найпоширеніших є використання банківських карток для отримання власних готівкових коштів а також операцій з переказів коштів на рахунки інших осіб. З одного боку, спрощується процес обігу грошових коштів, але в той же час, із використанням банківських карток зростають і ризики опинитися жертвою шахрайства.

Шахраї у сфері обігу банківських карток стали напрочуд винахідливими. Вже зараз виокремлюють навіть певні способи відповідних шахрайських дій: «скімінг», «траппінг», «фантом», «шаттер», «шиммінг», а також «трешинг», «фармінг», «фітинг». Однак без сприятливої для злочинця поведінки жертви, цей злочин вчинити майже неможливо. У даному випадку доцільно казати про «посередницьку» роль потерпідої особи у вчиненому правопорушенні. Віктимізації сприяє ціла низка факторів, головними з яких є неуважність осіб, їхня погана обізнаність, схильність до ризику та «психологія жадібності».

Отже, вважаємо доцільним запропонувати окремі заходи віктимологічної профілактики, які дозволять знизити кількість жертв від вказаного злочину:

– інформування осіб, що користуються послугами банків про всі можливі ризики та належні заходи безпеки (не повідомляти нікому персональних даних, не писати код на самій картці тощо);

– розміщення у банківських установах відповідних інформаційних стендів, які б роз'яснювали, як правильно використовувати банківські картки, як не стати жертвою шахрайства;

– розміщення цієї ж інформації на сайтах банків;

– запровадження інструктажу клієнтів працівниками банку стосовно на-

лежних дій у випадках виникнення будь-яких проблем у роботі з банкоматом чи при використанні банківської картки.

Таким чином, вважаємо, що наразі потребує вирішення низка нагальних проблем віктимологічної профілактики шахрайських дій із банківськими картками, однак вони потребують комплексного підходу, в тому числі, покращення загального рівня життя, соціального забезпечення, законодавчого врегулювання, врахування досвіду інших країн в галузі віктимологічної профілактики.

Література:

1. Пивоваров В. В. До питання латентності корпоративної злочинності в банківській сфері / В. В. Пивоваров // Науковий вісник Херсонського державного університету. Серія: Юридичні науки. – 2013. – Вип. 3, т. 2. – С. 104–106

2. Про платіжні системи та переказ коштів в Україні: Закон України від 05.04.2001 № 2346-III // Відом. Верхов. Ради України – 2001. – № 29.– Ст. 137

3. Стрєлков Л. О. Кримінальна відповідальність за незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення / Л. О. Стрєлков // Юридична наука. – 2011. – № 1. – С. 145-151

4. Сабадаш В. П. Фішинг як найбільш розвинений вид шахрайства в Інтернеті / В. П. Сабадаш // Університетські наукові записки. – 2006. – № 1. – С. 228-233

5. Афанасенко С. І. Особливості механізму віктимної поведінки жертв шахрайств / С. І. Афанасенко // Південноукраїнський правничий часопис. – 2014. – № 3. – С. 58-61

6. Попов К. Л. Некритичність і ризик як фактори підвищення віктимності при шахрайстві / К. Л. Попов // Вісник Академії адвокатури України. – 2015. – Т. 12, № 1. – С. 95–104

7. Антикібер. Незалежна асоціація банків України ваш захисник від кіберзлочинності [Електронний ресурс]. – Режим доступу: http://anticyber.com.ua/index.php