КРИМІНАЛЬНИЙ ПРОЦЕС І КРИМІНАЛІСТИКА

УДК 343.985

І.Л. Близнюк,
кандидат юридичних наук,
старший науковий співробітник

ВИЯВЛЕННЯ ТА РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ З НЕЗАКОННИМИ ОПЕРАЦІЯМИ З БАНКІВСЬКИМИ ПЛАТІЖНИМИ КАРТКАМИ (РЕКВІЗИТАМИ КАРТОК)

У статті розкриваються типові злочини, що вчиняються у сфері виготовлення та обігу банківських платіжних карток (БПК), проаналізовано особливості та виокремлено види вчинених шахрайств у зазначеній сфері в Україні. Особлива увага приділяється рекомендаціям оперативним працівникам та слідчим органів внутрішніх справ з виявлення та розслідування злочинів, пов'язаних з незаконними операціями з банківськими платіжними картками (реквізитами карток). Зокрема, у статті виокремлені основні напрями здійснення оперативного пошуку шахрайств, що вчиняються у сфері обігу БПК.

Ключові слова: *банківські пластикові (платіжні) картки, смарт-картки, чіпові картки, дистанційне банківське обслуговування, трансакції за картковими рахунками, шахрайства з платіжними картками, кіберзлочини, банкомати, ембосовані символи на картці, фітинг, "білий пластик", скіммер, ПІН-код, картоприймач банкомату, процесинговий центр, еквайр, POS-термінали, сервер, електронні журнали.*

В статье раскрываются типичные преступления, совершаемые в сфере изготовления и обращения банковских платежных карт (БПК), проанализированы особенности и выделены виды совершенных мошенничеств в указанной сфере в Украине. Особое внимание уделяется рекомендациям оперативным работникам и следователям органов внутренних дел по выявлению и расследованию преступлений, связанных с незаконными операциями с банковскими платежными картами (реквизитам карт). В частности, в статье отмечены основные направления осуществления оперативного поиска мошенничеств, совершаемых в сфере обращения БПК.

Ключевые слова: *банковские пластиковые (платежные) карты, смарт-карты, чиповые карты, дистанционное банковское обслуживание, трансакции по карточным счетам, мошенничества с платежными картами, киберпреступления, банкоматы, эмбоссированные символы на карте, фитинг, "белый пластик", скиммер, ПИН-код, картоприемник банкомата, процессинговый центр, эквайер, POS-терминалы, сервер, электронные журналы.*

Paper describes the typical crimes committed in the sphere of production and circulation of bank payment cards, analyzes the features of committing fraud in this field in Ukraine. Particular attention is given to the recommendations to operatives and investigators of the police in the detection and investigation of crimes related to the

illegal operations with bank payment cards (card details). In particular, the paper highlights key areas of operational search frauds committed in the sphere of circulation of bank payment cards.

***Keywords**: plastic bank (payment) card, smart card, chip cards, remote banking services, transactions on card accounts, payment card fraud, cybercrime, ATMs, embossed symbols on the card, fitting, "white plastic", skimmer and PIN–code, the card slot of the ATM, the processing center, acquirer, POS-terminals, server, e-journals.*

В Україні, як і у всіх розвинених країнах світу, на базі комп'ютерної системи електронного зв'язку широкого застосування набула міжбанківська система електронних платежів і взаєморозрахунків. Але вона не є абсолютно надійною. Нерідко на основі несанкціонованого доступу до комп'ютерних баз даних завдяки функціонуванню міжбанківської системи електронних платежів та взаєморозрахунків злочинці вчиняють незаконні операції з використанням банківських пластикових карток з корисливою метою та вчиняють шахрайство з використанням системи дистанційного банківського обслуговування. За даними НБУ, щоденно фіксуються десятки спроб несанкціонованого доступу до електронної системи міжбанківських розрахунків.

Збільшилась кількість несанкціонованих трансакцій за картковими рахунками, активно удосконалюються способи вчинення злочинів у сфері виготовлення та обороту банківських платіжних карток (БПК). Проте, за оцінками міжнародних експертів, розслідуються лише 15–20 % таких злочинів. Ця негативна тенденція пов'язана, з одного боку, з помилками та прорахунками банків при впровадженні БПК, а з іншого – з постійним удосконаленням механізму та способів учинення злочинів у сфері виготовлення та обігу платіжних карток, застосуванням найбільш завуальованих форм злочинної діяльності, поліпшенням технічної оснащеності і, як наслідок, – непідготовленістю правоохоронних органів ефективно протистояти таким злочинним проявам. У зв'язку з цим постає нагальна проблема щодо розробки ефективної методики виявлення та розслідування цього різновиду злочинів.

Найрозповсюдженими видами шахрайства з платіжними картками є шахрайство з підробленими картками, шахрайство з втраченими і викраденими пластиковими картками, шахрайство з картками, не отриманими законним держателем (за картками, які висилалися поштою і не були отримані клієнтом), шахрайство з використанням рахунку (операції без пред'явлення картки – в мережі Інтернет, телефонні або факсові замовлення), інші форми шахрайств.

Узагальнення практики боротьби з "картковою" злочинністю дозволяє класифікувати основні види правопорушень у сфері випуску та обігу БПК на такі групи:

• діяння, пов'язані з підробкою банківських платіжних карток, документів на переказ, придбанням, зберіганням, перевезенням, пересиланням з метою збуту, збутом підроблених банківських платіжних карток;

• шахрайські діяння з використанням банківських платіжних карток (використання інформації про справжні банківські платіжні картки (їх реквізити));

• діяння, пов'язані з незаконним збиранням інформації про справжні банківські платіжні картки.

Найбільше збитків – 39 % – банки несуть при підробці карток. На другому місці – операції без пред'явлення карток, тобто в мережі Інтернет [2].

Після переходу більшості європейських країн на чіпові картки (смарт-картки) як більш захищені основною тенденцією на європейському ринку стало

перетікання шахрайських операцій у віртуальне середовище. Не є винятком і Україна. Порівняно з 2011 р. цей показник за кількістю та сумами операцій зріс більш ніж у три рази [2]. У цілому, за офіційними даними НБУ, кожен другий український банк потерпає від шахрайських операцій.

Наприклад, у березні 2014 р. Ощадбанк попередив про активізацію шахрайських дій кіберзлочинців стосовно держателів платіжних карток як у банкоматних мережах вітчизняних банків, так і при розрахунках у мережі Інтернет. Так, останнім часом було зафіксовано випадки фітингу (технології онлайнового шахрайства, яка використовується зловмисниками для отримання особистої інформації користувачів), які полягали в спробах несанкціонованого отримання конфіденційної інформації держателів платіжних карток банку за допомогою шахрайських сайтів, що дублюють офіційні сайти відомих вітчизняних банків.

За офіційними даними НБУ, загальна кількість шахрайських операцій з БПК в 2012 р. порівняно з попереднім збільшилась на 47 %, а сума збитків зросла на 20 % [2]. При цьому 99,7 % збитків, заподіяних банкам за операціями з платіжними картками, здійснені з картками міжнародних платіжних систем.

Постійне збільшення цих цифр свідчить про наявність окремої підпільної індустрії, що пов'язана з незаконним виготовленням та використанням банківських пластикових карток. Тому не випадково питанням дослідження проблеми злочинних дій з використанням пластикових карток значну увагу приділили відомі вчені, зокрема Л.М. Стрельбицька, Л.В. Бистров, С.І. Ніколаюк, Г.А. Матусовський, А.В. Реуцький, В.Ю. Шепітько, О.В. Курман,

А.Ю. Ільницький, М.С. Вертузаєв, А.І. Котляревський, А.М. Юрченко та ін. Потреби оперативно-слідчої практики в розробці наукових положень і практичних рекомендацій щодо виявлення та розслідування злочинів, пов'язаних з незаконними операціями з банківськими платіжними картками (реквізитами карток), з одного боку, й відсутність сучасних монографічних досліджень цієї проблематики – з іншого, й обумовили актуальність обраної теми статті.

Найбільш гостро проблема шахрайств з банківськими платіжними картками постала в 90-ті роки з переходом фінансово-банківських структур на розрахунки з використанням електронних систем платежів.

Спочатку такі злочини вчинялися одинаками, сьогодні – організованими злочинними угрупованнями, інколи чисельністю до 50 чоловік, оснащеними найсучаснішою технікою. Такі угрупування користуються консультаціями висококваліфікованих фахівців, а для прикриття своєї протиправної діяльності мають надійні установчі документи.

Шахраї, які витіснялися з європейських країн у зв'язку з переходом міжнародних платіжних систем у межах боротьби із шахраями із магнітних карт на чіпові, змушені були звернути свою увагу на менш технологічні банківські ринки, і насамперед – на Україну, в якій склалася унікальна ситуація: величезна кількість випущеного пластику на тлі підвищеної уразливості як самих карток (із магнітною смугою), так і мереж передачі даних.

Характерним для злочинів, пов'язаних з використанням пластикових платіжних засобів, є їх висока латентність (90–95 %), "інтернаціональність", великі збитки, навіть від одиничного злочину, складність збирання доказів за встановленими фактами та доказування винуватості особи у вчиненні зазначеного кримінального правопорушення в суді.

Найбільш розповсюджені такі види шахрайств з банківськими платіжними картками.

1) Counterfeit Cards – дослівно перекладається як "фальшиві картки" – фізичне копіювання даних з магнітної смуги картки з подальшим записом на так званий "білий пластик". До недавнього часу це був найпоширеніший тип шахрайства з картками в нашій країні. Найчастіше цей вид злочинів вчиняється за допомогою скіммерів – спеціальних пристроїв, що встановлюються на картоприймач банкоматів. Одночасно може використовуватися псевдоклавіатура або відеокамера, які фіксують введення ПІН-коду.

Якщо раніше найпоширенішими були скіммери (ці пристрої слід було регулярно встановлювати та знімати), то тепер обладнання шахраїв передає дані бездротовими каналами зв'язку в режимі онлайн.

2) Card Stolen / Lost. На відміну від Counterfeit Cards, шахрайство Card Stolen/Lost полягає в проведенні операцій із загубленою або вкраденою картою.

3) Card Not Present – операції в Інтернеті. Використовується комп'ютерний вірус, що передає своєму власникові дані картки, які її утримувач використовує на своєму комп'ютері для різних розрахунків – поповнення мобільного телефону, оплати комунальних послуг тощо.

4) ID Fraud. Використовуючи систему ID Fraud, шахраї отримують платіжні картки за підробленими документами або через змову. Шахрай заволодіває документом, переклеює фото і звертається з підробкою в банк. Нерідко треті особи за певну винагороду відкривають за своїми документами картку та передають її третім особам.

Оперативний пошук ознак шахрайств, що вчиняються у сфері обігу банківських платіжних карток, здійснюється за трьома напрямами: виявлення фактів вчинення або підготовки злочинів; виявлення предметів та документів, що містять ознаки злочинної діяльності; виявлення осіб, які можуть бути віднесені до категорії підозрюваних, очевидців або потерпілих.

До основних установ, де можна отримати інформацію про вчинення зазначених кримінальних правопорушень або підготовку до них, відносяться:

- Національний банк України;
- процесинговий центр;
- платіжна система;
- банк-емітент БПК;
- еквайр;
- Українська міжбанківська асоціація членів платіжних систем "ЄМА".

Об'єктами оперативного пошуку є:

- особи, які в силу своєї діяльності (компетенція чи злочинна спеціалізація) мають можливість вчинювати злочини, пов'язані з використанням банківських платіжних карток;
- особи, які притягались до відповідальності за злочини, пов'язані з використанням банківських платіжних карток;
- особи, які можуть бути співучасниками при злочинних діях, пов'язаних з використанням банківських платіжних карток:
  - ❖ працівники банківських установ;
  - ❖ колишні працівники банківських установ;
- документи, в яких містяться ознаки злочинної діяльності;
- предмети (обладнання, об'єкти тощо), що можуть у подальшому виступати доказами за кримінальним провадженням.

Зокрема, органи внутрішніх справ здійснюють заходи, спрямовані на виявлення осіб, які так чи інакше пов'язані зі здійсненням будь-яких операцій із

застосуванням банківських пластикових платіжних карток. Таких осіб можна умовно поділити на дві категорії:

1. Працівники банківських установ: керівництво; технічний персонал; касири; інженери-програмісти (категорія, якій необхідно приділяти максимум уваги).

2. Колишні працівники банківських установ: звільнені через негативні причини; персонал, який мав доступ до комп'ютерних мереж, тощо.

Узагальнення слідчої практики дало змогу виокремити низку слідчих (розшукових), негласних слідчих (розшукових) дій, які найчастіше доручає слідчий органу дізнання при розслідуванні кримінальних правопорушень розглядуваної групи:

1) з'ясування нових епізодів злочинної діяльності;

2) з'ясування місця виготовлення підроблених банківських платіжних карток;

3) встановлення місцезнаходження грошових коштів та інших цінностей, отриманих злочинним шляхом;

4) виявлення каналів використання викрадених грошових коштів та інших цінностей;

5) встановлення конкретних учасників злочину, які входять в організовану злочинну групу, зв'язків між ними та ролі кожного при вчиненні злочинного діяння;

6) виявлення можливих співучасників, свідків, предметів та документів, що мають значення для справи;

7) одержання даних про причетність до злочину працівників банківських установ, процесингових центрів, підприємств, що обслуговують розрахунки банківськими платіжними картками, та ін.

З метою ефективного виявлення та розслідування злочинів зазначеної категорії необхідно наголосити, що місце події і місце злочину, як правило, не збігаються, оскільки злочин вчиняється в місцях обслуговування банківських платіжних карток, через POS-термінали або комп'ютери, а ознаки злочину виявляються безпосередньо в емітента платіжної картки або її власника. Місце події збігається з місцем злочину, якщо злочинця затримано в момент зняття готівки в банкоматі або при покупці товарів за платіжною карткою.

За злочинами у сфері виготовлення та обігу банківських платіжних карток огляд місця події здійснюється в приміщеннях:

а) підприємств, що обслуговують розрахунки банківськими платіжними картками, тобто там, де така картка була використана (магазини, кав'ярні, АЗС тощо);

б) де знаходиться банкомат, що використовується злочинцем для одержання грошових коштів;

в) банківських установ або процесингових центрів;

г) де виготовлялися підроблені банківські платіжні картки;

д) де встановлена комп'ютерна техніка, за допомогою якої було вчинено злочин, або знаходиться провайдер, що надає послуги з доступу в мережу Інтернет, а також на ділянках території, по яких проходять кабелі зв'язку між учасниками системи, що обслуговують обіг банківських платіжних карток.

Слід зазначити, що у зв'язку зі специфікою виготовлення та обігу банківських платіжних карток при проведенні огляду місця події необхідною умовою є залучення спеціалістів.

При цьому основними завданнями спеціалістів у галузі комп'ютерної техніки при огляді місця події є:

• виконання всіх маніпуляцій з комп'ютерною технікою (вмикання – вимикання, розбирання – складання та ін.);

• опис комп'ютерної техніки та периферійного устаткування в протоколах слідчих дій;

• проведення експрес-аналізу комп'ютерної інформації; виявлення інформаційних слідів злочину;

• запобігання знищенню або пошкодженню комп'ютерної інформації; вилучення комп'ютерної інформації та ін.

У зв'язку з тим, що всі події у сфері виготовлення та обігу банківських платіжних карток фіксуються процесинговим центром, сервером банківської установи, електронним контрольно-касовим апаратом, комп'ютерною технікою з POS-терміналом, важливо особливу увагу приділити вивченню файлів реєстрації на цих системах. Адже інформація про будь-яку подію (в тому числі, хто ініціював її, коли і в який час вона відбулася, які при цьому були порушені файли) реєструється в таких файлах. Зокрема, у файлах реєстрації може бути відображена інформація про паролі користувачів, їх імена, ідентифікаційні номери тощо.

Крім того, з метою ефективного виявлення та розслідування злочинів, що вчиняються з використанням БПК, працівниками ДСБЕЗ МВС України, що здійснюють оперативно-розшукову діяльність, вивчаються та перевіряються такі документи:

1) установчі документи підприємства, такі як статут, установчий договір, свідоцтво про державну реєстрацію суб'єкта підприємницької діяльності, свідоцтво про взяття на податковий облік тощо (у разі вчинення злочину шляхом створення підприємства та укладання з банківською установою договору на обслуговування банківських платіжних карток);

2) документи бухгалтерського обліку;

3) різні неофіційні документи (чернетки, розрахунки, списки банкоматів, реквізитів банківських платіжних карток);

4) аналітичні документи (довідки, звіти);

5) технологічні документи;

6) банківські документи (договори, додатки, роздруківки за рахунками, різні звіти, стоп-листи та ін.);

7) документи на машинних носіях інформації (електронні журнали, протоколи, реєстри);

8) різні касові документи (сліпи, квитанції банкоматів та POS-терміналів тощо).

Вважаємо за доцільне також з'ясувати таке:

1) призначення документа (БПК) і його справжність, визначити наявність або відсутність:

а) усі необхідні реквізити;

б) будь-які деформації БПК (зміна форми документа, сліди різних дій – наплавлення, хвилі, зафарбовування, відколи, зміни колірних відтінків, сліди нанесення різних речовин і т.ін.);

в) дефекти друку реквізитів;

г) відповідності реквізитів, які мають збігатися (при ембосуванні на платіжній картці знаки з одного боку вдавлені, а з другого боку опуклі);

д) відповідності розташування реквізитів;

е) відповідності барвників, паперу, захисної сітки, емблем та інших знаків (у тому числі голограми) встановленим тим або іншим стандартам;

є) збіг ембосованих знаків зі знаками, виконаними барвником;

ж) заміну ламінованого шару чи фотографій;

2) ознаки зміни БПК як у цілому, так і його окремих компонентів;

3) інформацію про особу або організацію, що відповідає за виготовлення, зберігання, випуск в обіг та використання БПК;

4) обставини, що мають значення для кримінального провадження;

5) мету та можливості використання БПК для здійснення тих чи інших операцій;

6) з якого матеріалу виготовлено БПК (наприклад, дослідити пластик банківської платіжної картки з вимірами його товщини, розміру, висоти ембосованих символів, перевірити справжність смуги для підпису власника), а також його реквізити, підписи, печатки, ембосовані символи;

7) кому видано БПК, його номер та дата випуску, строк дії.

При огляді сліпів, квитанцій POS-терміналів і банкоматів належить з'ясувати наявність обов'язкових реквізитів:

- ідентифікатора банківської установи;
- дату здійснення операції;
- вид операції (зняття, купівля чи повернення);
- суму операції (у гривнях чи іноземній валюті);
- реквізити банківської платіжної картки (визначені правилами безпеки платіжної системи);
- номер імпринтера POS-термінала чи банкомата, код авторизації;
- підпис касира (якщо це передбачено правилами платіжної системи);
- підпис держателя банківської платіжної картки (у випадку оформлення сліпа – обов'язково, а при оформленні квитанції платіжного терміналу – якщо це передбачено правилами платіжної системи).

Таким чином, криміногенна ситуація у сфері випуску та обігу банківських платіжних карток України залишається напруженою і має тенденцію до посилення ознак організованості вчинюваних злочинів. У зв'язку з цим актуальним є формування дієвих заходів щодо ефективного та своєчасного викриття та розслідування злочинів, пов'язаних з використанням БПК.

Вивчення практики боротьби зі злочинами у сфері випуску та обігу банківських пластикових карток дозволяє зробити висновок, що на сьогодні відчувається потреба в розробці науково обґрунтованих та практично значущих рекомендацій оперативним працівникам та слідчим органів внутрішніх справ відповідно щодо виявлення та розслідування таких кримінальних проваджень. Розробка зазначених методичних рекомендацій є вкрай необхідним завданням, оскільки кримінальні правопорушення у зазначеній сфері стрімко зростають та мають організований характер, при цьому постійно вдосконалюються способи вчинення злочинів цієї категорії, а заходи, що вживаються правоохоронними органами, як правило, не відповідають вимогам сучасності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Харчук М.В.* Аналіз масштабів та основні напрями мінімізації ризиків шахрайства членів міжнародних платіжних систем / М.В. Харчук [Електронний ресурс]. – Режим доступу : http : // www.economy.nayka.com.ua/?op=1&z=2120.

2. Кожен другий український банк потерпає від шахрайських операцій [Електронний ресурс]. – Режим доступу : http : // lohotron.in.ua/2013/02/kozhen-druhyj-ukrajinskyj-bank-poterpaje-vid-shahrajskyh-operatsij/.

3. Пірати XXI століття. Україна може стати оплотом шахрайства з платіжними картами [Електронний ресурс]. – Режим доступу : http : // lohotron.in.ua/2010/05/piraty-xxi-stolittya-ukrajina-mozhe-staty-oplotom-shahrajstva-z-platizhnymy-kartamy/.

Отримано 01.07.2014