

РАЗСЛЕДВАНЕ НА ПРЕСТЪПЛЕНИЯ, ИЗВЪРШЕНИ С ЕЛЕКТРОННИ ПЛАТЕЖНИ ИНСТРУМЕНТИ

проф. д-р Костадин Бобев*

Бургаски свободен университет

I. Исторически предпоставки за възникване на електронните банкови карти

1. Времето на появяването на първите банкови карти е свързано с възникването на кредитните платежни операции, които в началния период все още не са се осъществявали чрез банковите институции. Безспорен е фактът, че първите небанкови кредитни карти се появяват в САЩ, защото като подход и манталитет системата на кредитиране е най-широко разпространена в тази страна. В началото на 20 век в някои американски магазини започва издаването на пластмасови карти на своите богати клиенти, за да ги улеснят при извършването на покупки без налични разплащателни средства – банкноти и монети.

През 1928 г. Бостънската компания Farrington Manufacturing емитира първите метални пластинки, върху които са били шамповани (ембосирани) името и адреса на техните притежатели – кредитоспособни клиенти. Продавачите поставяли тези пластинки в специално устройство, наречено „импринтер“, което отпечатвало буквените и цифровите текстове от картата върху търговски чек, задължаващ клиента да внесе сумата в определен срок. По-късно били въведени някои облекчения за купувачите: едномесечен срок за погасяване на кредити, безлихвено кредитиране и други.

2. Общоприето е мнението, че началото на банковите кредитни карти е поставено от Джон Биггинс, шеф на кредитния отдел в Националната банка Flatbush в Бруклин, Ню Йорк. През 1946 г. Биггинс въвежда кредитиране по схема, наречена „Charge-it“, при която клиен-

* Професор, доктор на юридическите науки Костадин Бобев е работил в Научноизследователския институт по криминалистика и криминология при МВР повече от 42 години. 35 години е бил директор на този институт, участващ активно в разкриването и разследването на много тежки криминални и икономически престъпления. Автор е на десет монографии, 4 студии и над 100 научни публикации. В БСУ преподава две дисциплини – „Криминалистика“ и „Съдебни експертизи“.

тите давали в магазина специална разписка със стойността на покупката, след което продавачите ги изпращали в съответната банка за възстановяване на парите по сметката на клиента. През 1949 г. един от известните и влиятелни банкови специалисти Алфред Блумингдал, внук на основателя на най-големия американски универсален магазин пристига в Ню Йорк, където се среща със своя приятел Франсис Макнамар, шеф на финансовата компания Hamilton Credit Corp. За две години двамата инвестирали огромната за това време сума от 35.000 \$, която трябвало да промени организацията и системата за плащане на направените от постоянни посетители разходи в някои ресторанти, магазини и бензиностанции. Едва ли някои биха повярвали, че тази инвестиция може да се възстанови, ако не се е случило следното любопитно събитие. Блумингдал и Макнамар поканили на обяд своя експерт Ралф Спайдер в ресторант, близо до небостъргачите Емпайър Стейт Билдинг. По време на деловия разговор те се договорили да изготвят ембосирани карти за всички клиенти, ползващи ресторанта, околните магазини и бензиностанции. Нужни били обаче да се инвестират веднага тези 35.000 \$, за да може кредитната финансова компания да поеме ангажимент да продължи кредитното разплащане. Реално само Блумингдал внесъл 5.000 \$, след което се разделили. Макнамар и Спайдер с голям ентузиазъм започнали „реклама” на комплексната услуга като подпъхвали под вратите на съседни офиси листовки с описани за клиентите благоприятни условия. Даването на карта на конкретен клиент се преценявало по външния вид и поведение. Само за един месец Hamilton Credit Corp. получила при оборот от 2.000 \$ чиста печалба от 140,00 \$. Вторият месец бизнесът продължил да се разширява, печалбите нараствали и тримата приятели решили да организират сами познатия подход с кредитни карти в Лос Анджелис, където схемата била аналогична, но вече се наричала „Dine and Sign” (нахрани се и подпиши). Успехът бил неочакван. Само за три месеца в кредитната система били включени 25 ресторанта, а печалбата се увеличила двойно.

Тримата партньори се обединили на принципа „ако изгорим – да изгорим заедно”. Това обаче не се случило, защото за половин година печалбата в Ню Йорк нарастнала на 250.000 \$. Следващият град, който включили в „играта” бил Бостън. Така се поставило началото на известната банкова разплащателна система „Diners Club”, която през 1951 г. имала вече оборот от 6,2 милиона долара. Успоредно с развитието на американския пазар започнало интернационализирането на кредитните операции във Великобритания, където „Diners Club” получил лиценз. След това се появили днешните известни системи „American Express“, „Visa“, „MasterCard“ и други.

3. Първата кредитна карта на American Express, която е близка по вида на съвременните пластични разплащателни инструменти е била пусната на пазара на 01.10. 1958 г. Само след пет години банковата операционна система е обслужвала 32.000 фирми и 475.000 картодържатели. Увеличаващата се конкуренция между американските кредитни институции наложило тяхното обединяване, което станало през 1966 г. чрез създаването на междубанкова картова асоциация (ICA), която оказва положително влияние и на картовите системи в Европа, обединили се в Асоциация „EuroCard“. Това обединение създава благоприятни предпоставки и условия за внедряване на нови технологии и по-надеждни платежни операции. Паралелно с кредитните банкови системи в някои Западноевропейски страни като Великобритания, Швеция, Германия, Франция и Италия започва бързо внедряване на дебитните електронни системи за разплащане.

Развитието и разширяването на картовия пазар обаче, поставя основателно въпроса за оптималния финансов ресурс и гаранциите на банките относно неприкосновеността и защитата на паричните потоци на своите клиенти от престъпни манипулации, които ощетяват не само картодържателя, но и самите банкови институции.

II. Банковите карти – средство за извършване на престъпления

4. Злоупотребите с пластични банкови карти като разплащателен инструмент се наблюдава още в първите години на тяхното въвеждане. Увеличаващият се брой престъпления, свързани с използването на частично или изцяло фалшифицирани дебитни и кредитни карти стават сериозна заплаха за паричните активи на различни финансови институции и търговски обекти. От този сравнително нов вид престъпна дейност се засягат ежедневно голям брой национални и международни организации, респ. много граждани, претърпяли щети от измами с електронни платежни средства.

Успешното противодействие на тези престъпления е поставило пред специализираните органи и служители нови изисквания – добро познаване както на начините за изготвяне на недействителни платежни средства за отдалечен достъп, така и за методите, които използват престъпниците за придобиване на информация за данните на редовни банкови карти. На първо място, много важно е било да се знаят някои специфични понятия, свързани с банковите операции и платежните системи.

5. Видове електронни платежни инструменти.

Най-общо те се подразделят на две групи:

- платежни инструменти за отдалечен достъп;
- платежни инструменти за финансови разплащания с електронни пари.

Първият вид платежни средства дава възможност за получаване достъп до финансови средства по банкови сметки чрез: дебитна банкова карта, кредитна банкова карта и електронно банково платежно заявление (електронен способ за подаване на платежно заявление от титуляра на банковата сметка). **Вторият вид платежни инструменти** включва финансови операции чрез използване на електронни пари (парична стойност в е-форма), електронно банкиране (в реално време банката предоставя на своите клиенти дистанционен достъп до собствените им парични средства), електронна търговия (покупко-продажба на стоки и услуги без документ на хартиен носител), интернет банкиране и други.

6. Технически средства за безкасови плащания и лица, участващи в електронно-разплащателни операции.

6.1. Технически средства:

- ПОС терминално устройство (Point-of-sale terminal) за теглене на пари в брой (АТМ-банкомат) и автоматично устройство за плащане в търговски обекти;
- Автоматизирана система на **БОРИКА**, която е единственият оператор за банкомати в България. Тази система декодира и чете информацията върху магнитната ивица: № на картата (16-цифров код), държавата и банката, издател на картата, успешните и неуспешни транзакции на суми;
- Електронна система на банката, която издава картата.

6.2. Физически лица, участващи при въвеждане на данни за безкасово плащане: при транзакция на ПОС терминала съответното служебно лице автоматично въвежда данни за № на банковата карта от магнитната лента чрез прекарване през четец, а собственикът на картата – за сумата за плащане и ПИН кодът чрез бутони на клавиатурата на ПОС терминала.

7. Електронни карти и елементи за тяхната защита.

Според притежателя електронните платежни инструменти биват три вида: за физически лица, за юридически лица и за богати хора, чиято платежоспособност е гарантирана (персонални карти). Независи-

мо от вида и предназначението електронните банкови карти **имат следните задължителни атрибути**, които гарантират тяхната автентичност:

- 15 или 16 цифров номер на сметката, който за различните фирми, издатели на картата започва с определено число. Така например за „Виза” е 4, за „Мастър Кард” – 5, за „Американ Експрес” – 37, за „Дайнърс Клъб” – 38 и т.н.;
- срок за валидност на картата върху лицевата страна;
- име на собственика (картодържателя);
- буквена сигнатура за копиране (MC, CV, At Ex и др.);
- фигурки или обозначения върху полето за подпис на картодържателя (на обратната страна на картата), които при осветяване с УВ светлина луминисцират. Например за „Виза” е лелящо гълъбче, при „Мастер Кард” – буквите MC и т.н.;
- магнитна лента, холограма, микро-чип и др.

Елементите на лицевата и обратната страна на една електронна банкова карта, издадена в България се определят и разполагат съгласно специална Наредба на БНБ. Всеки издател на банкови карти е длъжен да включи като реквизит върху лицевата или обратната страна на картата логото на Националния оператор (видимо или закодирано).



Масовият картов продукт, който се издава у нас са националните дебитни карти с логото на БОРИКА – жълто лъвче на зелен фон и начални цифри, започващи с 67. Това лого гарантира възприемането на картата от всяко терминално устройство, свързано със системата на Националния оператор. С българските дебитни карти могат да се извършват шест вида операции:

- теглене на пари в брой чрез банкомати (АТМ);
- заплащане на стоки и услуги;
- разплащания чрез Интернет;
- плащания на услуги чрез терминални устройства (АТМ);
- преводи по сметки чрез АТМ;
- справочни платежни и неплатежни операции.

III. Начини за извършването на престъпления чрез използване на истински или подправени електронни платежни инструменти

8. Престъпниците използват различни начини и технически средства за реализиране на своите престъпни намерения:

8.1. Най-лесният начин за извършване на престъпление е използването на истинска дебитна или кредитна карта без знанието на законния картодържател. Това става обикновено от членове на семейството, роднини или от лице, което е намерило банковата карта, и върху която картопритежателят е записал ПИН кода, за да не го забрави.

8.2. Използване на различни устройства-приставки, наподобяващи „самоделен джоб“, които се поставят в отвора за прием на карта в банкомата. Този начин, наречен „ливанска примка“ цели да блокира изваждането на платежния инструмент. Докато лицето се суети се явява „случайно преминаващ гражданин“, който предлага своята услуга, но трябва да знае ПИН кода. След няколко несполучливи опита „помагачът“ препоръчва на лицето да отиде до банката и поиска съдействие. През това време той изважда примката, въвежда ПИН кода и изтегля максимално допустимите парични средства. Измамите с „ливанска примка“ стават обикновено в късния петъчен следобед, когато банките вече са затворени и престъпниците могат да теглят суми в събота, неделя и първите часове на понеделник.

8.3. Разновидност на „ливанска примка“ е „алжирско V“, при което се използва елементарен механизъм, представляващ магнитна лента от магнитофонна касета, която допълнително е приспособена да блокира изваждането на картата. След като картата е задържана, действията се развиват както при „ливанска примка“. При разследване на

престъпления, извършени с описаните два способа е установено, че престъпниците предварително залепват на банкомата телефонен номер на някои от групата измамници, посочен за „съдействие”, който при позвъняване се представя за служител на банката, успокояващ картодръжателя, че сметката веднага ще бъде блокирана, а техническият проблем на банката ще бъде отстранен.

8.4. Разпространен начин за кражба на информация от магнитните ленти на истински банкови карти е чрез монтиране на специално устройство, наречено „скимер”. Това устройство се въвежда в жлеба на АТМ, предназначен за поемане на банковата карта. Устройството се хранва с батерии, което изисква повече време за инсталиране. Затова престъпниците подбират АТМ, които са без видеонаблюдение и физическа охрана. Съвременните „скимери” могат да „откраднат” съхранявана информация от 400 банкови карти.

8.5. Не са редки случаите, когато научаването на ПИН кода на банковата карта става чрез:

- микрофонен запис на комбинация от звуци (съответстваща на отделните цифри от 0 до 9) при набиране на ПИН кода;
- надничане или използване на огледало от съседен магазин, офис, паркиран автомобил и др. близки обекти;
- заснемане с монтирана наблизо фото- или видеокамера;
- поставяне на фалшива двойна клавиатура, която позволява на картопритежателя да тегли пари, но едновременно с това да се записва използвания от него ПИН код.

8.6. Изготвяне на фалшиви електронни платежни инструменти, чрез използване на:

- бели пластики с размери на оригинални карти, върху които има само магнитна лента;
- неистински пълни копия, които се изготвят чрез полиграфски печат и последващо имитиране на защита (холограми, лого, цветове и др.);
- истински банкови карти, които след загубване или кражба се преправят от престъпниците с последващо нанасяне на определена информация. Обикновено това става с „енкодер” (устройство, записващо информация от специализиран софтуер върху магнитната лента).

IV. Разкриване и разследване на престъпления, извършени с електронни карти

9. При разкриването и документирането на този вид престъпления се срещат определени затруднения, главно поради специфичните особености на подготовката и начина на извършване на престъпното деяние. Обикновено при тези престъпления няма свидетел извън кръга на пострадалите лица. Характерна особеност на престъпленията с разплащателни карти е използването на т.н. „продукция с възможна двойна употреба“ – карти с магнитни полета, микрочипове, звукови и цифрови файлове, микропредаватели, „четци“ на магнитни карти и други, които свободно се продават в търговската мрежа. Тези устройства намират приложение в много други области на радиоелектрониката и компютърните технологии.

Много важно в такива случаи е събирането на различни доказателства с участието на подготвени специалисти, назначаване на експертизи, прилагане на специални разузнавателни средства, подобряване качеството на заснети с охранителни камери лица, извършващи престъпление с банкови карти.

10. От различните способности за доказване важна роля имат няколко от тях:

10.1. *Претърсване и изземване.* Това е класически способ за събиране и проверка на доказателствен материал, който в тези случаи трябва да се извършва задължително в присъствие на компютърни специалисти и поемни лица, съблюдаващи законосъобразността на действията на следствено-оперативната група и процесуалното изземване и фиксиране на откритите устройства и технически принадлежности. Като способ за доказване, претърсването и изземването почти винаги се предшества от разпит на свидетели и назначаване на експертизи.

10.2. *Назначаване и извършване на съдебни експертизи.* Най-често в тези случаи се назначават комплексни експертизи – технически, компютърни и криминалистични. Специализираните лаборатории и вещите лица, подготвени за този вид експертизи са служители на Научноизследователския институт по криминалистика и криминология (НИКК) при МВР, Научно-техническите лаборатории (БНТЛ и НТЛ) при Областните дирекции на МВР, Техническите университети в София и страната, БАН и други. Въпросите, които решават тези лаборатории са от различни научни области, но целите и задачите са насочени към даване на изчерпателен отговор за начините за извършване на престъпленията с платежни електронни средства, за нанесените материални и морални щети, за

извършителите и тяхната организираност. Най-често пред вещите лица се поставят следните въпроси:

- Какво представляват иззетите от обвиняемия (уличения) технически устройства, системи и детайли, изправни ли са и годни ли са за използване по предназначение?
- Какви програми са инсталирани във вътрешната памет на иззетия компютър и какво е тяхното предназначение?
- Има ли информационни файлове, които да съдържат цифрови данни, съответстващи на световните и националните стандарти за банкови карти?
- Върху иззетите фалшиви банкови карти и технически средства има ли дактилоскопни следи от ръце и биологичен материал, годен за ДНК профилиране и идентифициране на лицата, които са ги оставили при пипане на инкриминираните обекти?
- Върху иззетите писмени документи има ли текстове с буквени и цифрови обозначения, използвани при генериране на кодовете на съответните карти, чрез които да се идентифицират авторите на текстовете!

Данните от експертизите и разпитите на свидетели могат да се проверят чрез организиране и провеждане на следствен експеримент и разпознаване на лица и предмети.

10.3. Приложение на специални разузнавателни средства. Това е много ефективен способ за доказване на престъпната дейност с фалшифицирани платежни електронни инструменти. Особено голямо значение има този способ при доказване престъпната дейност на организирани групи, създадени с единствената цел да използват неистински или преправени електронни карти за извършване на крупни финансови закононарушения. Полицейската и съдебната практика показват, че при използване на видеонаблюдение на банкомати, голям процент от заснетите лица, извършили неправомерни манипулации пред АТМ се разкриват, идентифицират и осъждат. Разбира се, категоричното доказване на престъпната дейност на лицата става със съдействието на Националния оператор “Борика”, от който се получава информация за неправомерно изтеглени суми с преправени дебитни и кредитни карти.

11. Превантивни действия за предотвратяване и пресичане на престъпления с електронни разплащателни средства.

Към всички картодържатели – граждани и институции могат да се направят следните препоръки при използване на банковите карти:

- Банковата карта не трябва да се предоставя на други лица, независимо от близостта и доверието!

- Ако ПИН кодът е записан върху лист, той не трябва да се носи заедно с картата!
- При блокиране на картата в банкомата, трябва незабавно да се телефонира на банката-картоиздател! За целта указаният телефонен номер трябва да се държи на достъпно място!
- След изтегляне на пари от банкомат, получената разписка не трябва да се изхвърля в близост до банкомата!
- При въвеждане на ПИН в АТМ е желателно със свободната ръка да се прикрива клавиатурата!
- Състоянието на личната банкова сметка трябва да се проверява периодично. Недопустимо е изпращането на лични данни, пароли и номера на банкови карти и сметки чрез съответния e-mail адрес.
- Всички on-line услуги, търговия и банкиране, които изискват писмено изпращане на информация трябва да се правят след съгласуване с представител на банката по Интернет или след среща в негов банков офис!
- При нужда от информация или съвет правилно е да се потърсят риск-мениджърите на MasterCard и Visa, отговарящи за районите, в които попада България.

Литература

1. Бобев, К. Криминалистика, Университетско издателство „Св. Кл. Охридски”, София, 2009 г.
2. Бояджиева, Ю., Трайкова, Е. Престъпност в сферата на електронните платежни инструменти, изд. МВР, София, 2010 г.
3. Пенев, Й. и колектив. Методика за разкриване и разследване на престъпления с електронни банкови карти. Академия на МВР, Асоциация на полицейските началници. Генерална дирекция „Полиция”, София, 2006 г.
4. Гинзбург, А.И., Пластиковъте картм, изд. „Питер”, Москва, 2004 г.

РЕЗЮМЕ

Престъпленията свързани с електронни платежни инструменти са актуален проблем в съвременното общество. Използването на разплащателни банкови карти за различни финансови операции може да бъде компрометирано от недобросъвестни лица, стремящи се към материални облаги, придобити по незаконен и престъпен начин.

В статията авторът прави исторически преглед на появяването и утвърждаването на кредитните и дебитните карти в САЩ и света, на усилията за непрекъснато усъвършенстване на защитите на информационните данни, заложен в тях и на превантивните мерки за предотвратяване и пресичане на престъпленията с тези платежни инструменти. Специално внимание е отделено на особеностите при разследване на престъпления с банкови карти и приложението на различни методи за доказване на извършителите на тази престъпна дейност.

S U M M A R Y

Criminal acts closely associated with electronic payments, such as credit or debit cards, are becoming prevalent in our present-day society. The use of such payments can be easily compromised by unscrupulous individuals seeking materialistic benefits obtained through illegal conducts.

In the article, the author examines the history behind the establishment of the credit and debit cards in the US and the world, as well as the reasons behind their increasing popularity as methods of payment. The article further describes the constant efforts that are being put in place in order to secure personal information, in addition to observing the methods taken to prevent criminal acts that compromise these electronic tenders. Special attention is devoted to the distinct practices that police and governments employ to catch individuals who are involved in such criminal activities.