

адміністративні правовідносини, що виникають у сфері обігу вогнепальної зброї, і, насамперед, підвищувати ефективність діяльності органів дозвільної системи, інших правоохоронних органів, наділених державно-владними повноваженнями щодо ухвалення відповідних рішень, здійснення контролю, проведення відповідних профілактичних заходів тощо.

**~Skimming – фінансові злочини, пов'язані
із використанням банкінгу~**

**~Skimming – przestępstwa finansowe związane
z bankowością elektroniczną~**

Маліновська І. (Malinowska I.), старший викладач Інституту досліджень організованої злочинності та тероризму Вищої школи поліції в м. Щитно (Республіка Польща), підінспектор поліції

Піатковська Б. (Piątkowska B.), викладач кафедри безпеки Вищої школи безпеки в Познані (Республіка Польща), підінспектор поліції

У дослідженні проаналізовано використання фінансових злочинів, у тому числі й пов'язаних із використанням банкінгу із суміжними сферами, зокрема торгівлею людьми, наркотрафіком, торгівлею зброї. Розкрито термінологічну базу, приділено увагу законодавчому забезпечення протидії злочинам у досліджуваній сфері.

Wstęp

Bardzo wyraźny rozwój nowoczesnych technologii w ostatnich trzech latach oraz związane z tym rozwój elektronicznych form płatniczych – pomimo iż niesie za sobą wiele korzyści – to stał się również impulsem dla zorganizowanych grup przestępczych, których działania

polegają na okradaniu kont bankowych.

Jednym z najbardziej rozpowszechnionych, a zarazem najniebezpieczniejszym przestępstwem związanym z użyciem kart płatniczych, jest tzw «skimming».

Skimming jest przestępstwem polegającym na bezprawnym skopiowaniu danych znajdujących się na pasku magnetycznym karty płatniczej oraz przechwycenie kodu PIN (bez wiedzy i woli posiadacza), celem wytworzenia duplikatu karty płatniczej. Tego rodzaju karta działa identycznie jak karta oryginalna, a transakcje nią dokonane obciążają jej posiadacza.

Dokonywane transakcje z jej użyciem są często niemożliwe do wykrycia, ponieważ wykonywane są przez międzynarodowe gangi skimmerów w różnych stronach świata. Wymieniają się oni – poprzez sieć internetową – zawartością pasków magnetycznych z oryginalnych kart.

Definicja karty płatniczej

Definicja karty płatniczej została określona w ustawie z dnia 19 sierpnia 2011 r. *o usługach płatniczych* [1] - w dyspozycji art. 2 pkt 15 a podano, iż jest to: *karta uprawniająca do wypłaty gotówki lub umożliwiająca złożenie zlecenia płatniczego za pośrednictwem akceptanta lub agenta rozliczeniowego, akceptowana przez akceptanta w celu otrzymania przez niego należnych mu środków.*

Najogólniej mówiąc – karta płatnicza (z ang. payment card) zawiera cztery istotne elementy, które charakteryzują ją jako instrument płatniczy – tj.:

- jest standardowa – standardy reguluje akt ISO 7810; posiada wymiary: wysokość - 53,98 mm, szerokość - 85,6 mm i grubość – 0,76 mm,
- jej wystawcą jej odpowiednia instytucja (najczęściej bank),
- jest włączona do jednego z systemu rozliczeń, np. VISA,
- płatności dokonywane za jej pomocą muszą być akceptowalne.

Służy ona do regulowania płatności za usługi i nabyte towary oraz do podejmowania pieniędzy z bankomatu – czyli

za jej pomocą można dokonywać bezgotówkowych transakcji płatniczych. Wyposażona jest w pasek magnetyczny lub chip, na którym zapisywane są informacje o posiadaczu karty (imię i nazwisko), nazwa banku, identyfikator karty oraz jej data ważności.

Rodzaje kart płatniczych

W literaturze przedmiotu istnieje wiele metod klasyfikacji kart płatniczych. Najczęściej dzieli się je, z uwagi na sposób dokonywania płatności [2]:

- *karta kredytowa* – jest to karta, której uzyskanie nie jest związane z posiadaniem rachunku bankowego. Posiadacz tej karty bazuje na limicie kredytowym przyznanym przez bank;

- *karta debetowa* – karta służy do wykonywania transakcji płatniczych i jest powiązana z rachunkiem bankowym posiadacza. Za jej pośrednictwem można dokonać wypłaty z bankomatu. Właściciel karty musi posiadać odpowiedni stan środków na koncie, aby transakcje były przeprowadzane bez żadnych problemów. Ponadto saldo dostępnych środków jest powiększone o dostępny limit zadłużenia, czyli tzw. debet (z ang. debit);

- *karta obciążeniowa*, z tzw. odroczonym terminem płatności. Jest ona zmodyfikowanym rodzajem karty kredytowej. Aby otrzymać tego rodzaju kartę, należy posiadać w danym banku rachunek przez określony czas. Bank określa – na podstawie miesięcznych wpływów – limit środków, które może udostępnić posiadaczowi. W tym przypadku odroczone płatności polega na tym, występuje konieczność spłacania kredytu przez płatności kartą w najczęściej miesięcznych odstępach czasu;

- *karta bankomatowa* karta służąca jedynie do dokonywania wypłat gotówki z bankomatu czy też innego urządzenia z funkcją wypłaty gotówki i dokonywaniu innych operacji bankowych. Praktycznie karta ta nie występuje już w obrocie;

– *karta przedpłacona – typu prepaid* – środki pieniężne znajdujące się na karcie, są zakodowane w postaci tzw. impulsów – nie są ulokowane na rachunku bankowym. Karty tego rodzaju mogą być wydane na okaziciela (czyli nie są związane z konkretną osobą) i mogą być wykorzystywane jako np. karty podarunkowe;

– *karta wirtualna* – karta ta nie jest wydawana w postaci fizycznej. Istnieje ona jako numer rachunku bankowego, który jest wykorzystywany do płatności dokonywanych za pośrednictwem Internetu.

W literaturze przedmiotu spotykać się można z jeszcze innymi kryteriami podziału kart płatniczych. Są następujące klasyfikacje:

a) Z uwagi na technologię zapisu na karcie [2]:

– *karta tłoczona* – dane posiadacza karty naniesione są poprzez wytłoczenie lub wykonanie termodruku; karta ta wychodzi z użycia;

– *karta magnetyczna* - dane o karcie, jak i o jej posiadaczu zapisane są na pasku magnetycznym; są one coraz częściej zastępowane przez karty mikroprocesorowe;

– *karta mikroprocesorowa (mikrochipowa)* – w przypadku tej karty dane o posiadaczu karty, jak i o niej samej, zawarte są w mikroprocesorze wbudowanym w kartę; oferuje ona większą funkcjonalność i pojemność;

– *karta hybrydowa* - wszystkie dane o niej samej oraz o posiadaczu karty są zapisywane równolegle w mikroprocesorze, jak i na pasku magnetycznym.

b) Z uwagi na marketing: 1) karty klasyczne (standardowe karty płatnicze); 2) karty srebrne (Silver) – przeznaczone dla osób o wyższym poziomie dochodów; 3) karty złote (Gold) – karty dla osób o wysokich dochodach i gwarantują zwolnienia z opłat; 4) karty platynowe (Platinum) – przeznaczone dla zamożnych osób i zapewniają dodatkowe usługi; 5) karty ekskluzywne – karty dla VIP-ów, oferują najszerszy zakres usług.

c) **Z uwagi na logo organizacji płatniczej, znajdujące się na karcie:** VISA, MasterCard oraz mniej popularne w Polsce, ale znane i cenione w świecie - American Express i Dinners Club.

Przestępstwa z użyciem kart płatniczych

Najczęstszymi rodzajami przestępstw związanych z obrotem kartami płatniczymi (tzw. fraudulent transaction) – są [3]:

- *posługiwanie się skradzionymi lub zagubionymi kartami* – sprawca po wejściu w posiadanie karty w wyniku np. kradzieży przywłaszczenia, podszywa się pod jej właściciela i stara się dokonać jak najszybciej transakcji karta aktywną;

- *wyludzenie kart płatniczych na podstawie wniosku zawierającego fałszywe dane bądź wystawionego na podstawioną osobę* – złożenie wniosku z fałszywymi danymi do banku celem otrzymania oryginalnej karty płatniczej. Na podstawie otrzymanej karty przestępcy dokonują początkowo transakcji na duże kwoty, a następnie wypłat powyżej limitów autoryzacyjnych;

- *wykorzystywanie kart podrobionych (sfalszowanych)* - pokrzywdzonym jest zarówno posiadacz karty, jak i emitent karty płatniczej; fałszowanie polega na: podrobieniu karty, jej przerobieniu, całkowitym sfalszowaniu oraz fałszerstwie elektronicznym;

- *kopiowanie kart płatniczych na rachunkach obciążeniowych* – fałszowanie dowodów transakcji przez nieuczciwych akceptantów; ujawnienie tego przestępstwa wymaga współpracy z posiadaczem karty i posiadania przez niego oryginału rachunku obciążeniowego;

- *wykorzystanie danych cudzej karty (carding)* – nieupoważnione posługiwanie się danymi z karty, uzyskanymi np. poprzez fizyczny kontakt z posiadaczem karty, za pośrednictwem Internetu, itp.;

- *wyludzenia towarów i usług przez legalnego posiadacza karty* - posiadacz kupuje towar i usługę, ale za nią nie płaci,

gdyż celowo zmienia miejsce pobytu, nie informuje o tym wydawcy karty i nie zwraca mu jej karty;

– *phising* - oszustwo polegające na kradzieży tożsamości. Przestępca podszywa się pod znane adresatowi osoby i firmy, celem wyłudzenia od niego informacji takich jak, np. danych logowania do bankowości internetowej, nakłonienia go do wykonania określonych działań, itp.

Skimming - rodzaje

Skanowanie kart ma najczęściej miejsce podczas transakcji dokonywanych w bankomatach, jak również możliwe jest podczas dokonywania zapłaty w sklepach czy restauracjach, na stacjach benzynowych. Wyróżnia się dwa rodzaje skimmingu:

Skimming w placówce handlowo-usługowej

Jest to rzadziej spotykana forma przestępczości w tym zakresie. Proceder ten polega na skopiowaniu paska magnetycznego przez sprzedawcę, który współpracuje z przestępcami lub sam działa przestępczo. Najczęściej jest w posiadaniu karty przez krótki czas i nie zawsze może poznać kod PIN. Stąd też z reguły kopiowane są karty nie wymagające autoryzacji przy pomocy PIN-u. Kopiowania zawartości pasków magnetycznych dokonuje za pomocą skimmera – jest to małe urządzenie, które zawiera czytnik kart oraz pamięć. Powyższe urządzenie podłączane jest do komputera i następuje kopiowanie zawartości nielegalnie przechwyconych pasków magnetycznych.

Skimming bankomatowy - zwalczanie

Tego rodzaju proceder polega nielegalnym kopiowaniu informacji zawartych na karcie płatniczej celem wykonania jej kopii oraz dokonywanie wypłat za jej pomocą z rachunku bankowego posiadacza oryginalnej karty.

Mechanizm działania przestępców w tym zakresie wygląda następująco:

– **Po pierwsze** – umieszczają na bankomatach urządzenia skanujące, tzw. skimmery i za ich pomocą kopiuja dane z kart. Urządzenia te, to nakładki, które umieszczają na

otworze, do którego wsuwa się karty. Dzięki temu skanują zawartość paska magnetycznego karty płatniczej i nagrywają uzyskane dane na oryginalne karty płatnicze bądź na kawałek plastiku z paskiem magnetycznym (tzw. białą kartę – white plastic) lub przesyłają je do umieszczonego w niewielkiej odległości czytnika, który je zapisuje. Skimmery trudno dostrzec, gdyż są dobrze dopasowane i w tym samym kolorze co bankomat.

– **Po drugie** – aby uzyskać kod PIN, oszuści montują (w specjalnie dopasowanym banerze reklamowym bądź w listwie z logo systemów kart płatniczych) nad klawiaturą nakładkę z mini kamerą, która rejestruje rękę osoby wstukującej numer. Osoba dokująca operacji, nie dostrzega żadnej różnicy w funkcjonowaniu bankomatu.

Najczęściej po kilkunastu godzinach – po demontażu urządzenia z bankomatu - przestępcy przenoszą w formie elektronicznej do komputera dane uzyskane ze skimmera i kamery; dane te przesyłają w dowolne miejsce w kraju lub na świecie. Nielegalnie zdobyte informacje nagrywane są na karty z paskami magnetycznymi i używane jako prawdziwe.

Jest wiele sposobów walki z omawianym procederem. Poniżej przypadki:

– Niektóre banki w swoich bankomatach posiadają funkcję, która powoduje, że po włożeniu karty płatniczej wibruje ona. Tego rodzaju mechanizm ma ją zabezpieczyć przed czytaniem danych.

– Jeszcze inne zabezpieczenia, to plastikowe wypustki znajdujące się wokół otworu na kartę; uniemożliwia to zamontowanie przez przestępców skimmera.

– Wielu posiadaczy kart płatniczych posiada karty z wbudowanym chipem – ma on być zabezpieczeniem przed nieuprawnionym sczytaniem danych przez przestępców. Otóż - informacja o chipie zapisana jest na pasku magnetycznym i w sytuacji, gdy bankomat czyta informację, uruchamia się moduł EMV [4], który łączy się z chipem. Następnie na wyświetlaczu bankomatu włącza się komunikat, że wydłużony

będzie czas oczekiwania na przeprowadzenie danej operacji. Z taką zeskimmowaną kartą z chipem przestępca nie będzie mógł jej użyć w bankomacie obsługującym moduł EMV.

Zakończenie

Pomimo wielu zabezpieczeń ze strony banków przed skimmingiem, przestępcy w sposób skuteczny korzystają z nowoczesnych technologii i czasami mogą się one okazać niewystarczające.

Z tego też względu sami posiadacze kart winny zachowywać czujność w trakcie korzystania z bankomatu i w przypadku jakichkolwiek podejrzeń, przekazywać informacje o nieprawidłowościach pracownikom banków czy też funkcjonariuszom Policji.

Podsumowując – można wyróżnić trzy zasadnicze metody zwalczania skimmingu [2]:

- zwiększenie poziomu technologicznego zaawansowania zabezpieczeń kart płatniczych, a także urządzeń służących do ich obsługi, tj. m.in. bankomatów i terminali płatniczych,
- edukacja uczestników obrotu kartami płatniczymi, czyli posiadaczy kart płatniczych i akceptantów,
- działania instytucji zajmujących się zwalczaniem tego procederu – tj. Policji oraz banków.

Bibliografia:

1. Miklaś K., Pawlak M., Zastosowanie kart elektronicznych w systemach płatniczych, Politechnika Poznańska – Systemy informatyczne w zarządzaniu 2013/2014, http://www.mcp.poznan.pl/wp-content/uploads/2014/12/2013_14_zimowy_94342i94356_Zastosowanie-kart-elektronicznych-w-systemach-p%C5%82atniczych.pdf, z 6 kwietnia 2015 r.
2. Mikołajczyk K., Przestępstwa związane z wykorzystaniem bankowości elektronicznej – skimming, Przegląd Bezpieczeństwa Wewnętrznego 10/14, s. 105 – 106, [file:///C:/Users/R540/Downloads/Segregator_5%20\(3\).pdf](file:///C:/Users/R540/Downloads/Segregator_5%20(3).pdf), z 1 kwietnia 2015 r.
3. Przestępstwa z użyciem kart płatniczych, <http://www.kartyplatnicze.info/przestepstwa.php>, z 4 kwietnia 2015 r.
4. Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych, tekst jednolity – Dz. U. z 2014 r., poz. 873, z późn. zm.