Mgr Izabela Sękowska
Komenda Wojewódzka Policji w Olsztynie

KRYMINALISTYCZNE ASPEKTY SKIMMINGU BANKOMATOWEGO

Streszczenie

Skimming bankomatowy to przestępstwo, które w Polsce występuje coraz częściej. Czyn ten polega na kopiowaniu kart bankomatowych, uzyskiwaniu kodów PIN a następnie wytwarzaniu fałszywych kart służących do pobierania wypłat z rachunków ich nieświadomych właścicieli. Popełnienie skimmingu wymaga współpracy przynajmniej kilku osób, dlatego jest on domeną przestępczych grup zorganizowanych. Zwalczanie skimmingu bankomatowego wymusza współpracę Policji z przedstawicielami banków. Analizę przestępczego sposobu działania oparto na dwóch przykładach skimmingu bankomatowego, wykrytego przez Policjantów Wydziału do Walki z Przestępczością Gospodarczą Komendy Wojewódzkiej Policji w Olsztynie. Występowanie aspektów kryminalistycznych w przedstawionym tekście zaznacza się w ustalaniu *modus operandi* oraz roli ekspertyzy kryminalistycznej w wykrywaniu.

Słowa kluczowe: skimming, bankomat, kopiowanie kart, nielegalne kopiowanie, bankowość elektroniczna, karta, nakładka.

FORENSIC ASPECTS OF SKIMMING ATMs

Abstract

Skimming is a crime, which in Poland is more and more often. This act involves copying ATM cards, obtaining the PIN and then the production of counterfeit cards designed to collect payments from the accounts of their respective owners. This act requires the cooperation of at least a few people, so they do it by organized crime groups. Fighting skimming ATMs police forces cooperate with representatives of the banks. Analysis of the criminal *modus operandi* of criminals based on two examples skimming ATMs were detected by the Police

Department for Fighting Economic Crime Police in Olsztyn. Occurrence factors forensic presented in the text indicates the determination of the modus operandi and the role of forensic detection.

Keywords: skimming, ATM, card copy, illegal copying, electroning banking, card, frontend.

„Doskonałe bezpieczeństwo i nietykalność własności oraz osoby: oto prawdziwa wolność społeczna."
Antoine Rivarol

Wprowadzenie

Przestępstwo skimmingu bankomatowego jest jednym zagrożeń bankowości elektronicznej, ponieważ narusza bezpieczeństwo obywateli w miejscach publicznych. Bankowość elektroniczna (e-banking) to formą usługi, która polega na umożliwieniu uprawnionego dostępu do rachunku bankowego za pomocą urządzenia elektronicznego takiego jak komputer, bankomat, telefon, terminal lub linia telekomunikacyjna[1]. Ważną rolę w tym pełni karta płatnicza. Jest ona instrumentem płatniczym, który identyfikuje wydawcę i upoważnionego posiadacza, uprawniając do wypłaty gotówki lub dokonywania zapłaty, a w przypadku karty wydanej przez bank lub instytucję ustawowo upoważnioną do udzielania kredytu – także do dokonywania wypłaty gotówki lub zapłaty z wykorzystaniem kredytu[2].

Pierwsze bankomaty akceptowały papierowe karty, kupowane uprzednio w banku. Po przeprowadzeniu transakcji urządzenie zatrzymywało taką kartę[3]. W Polsce banki wypuściły pierwsze karty z początkiem lat dziewięćdziesiątych ubiegłego wieku. Były to proste karty z ograniczoną funkcjonalnością. Jednak już po kilku latach banki zaoferowały przeróżne możliwości kartowe, a liczba wydanych kart liczyła miliony[4].

---

[1] G. Szwajkowska, P. Kwaśniewski, K. Leżoń, F. Woźniczka, *Usługi bankowości elektronicznej dla klientów detalicznych, charakterystyka i zagrożenia*, Urząd Komisji Nadzoru Finansowego, Warszawa 2010, s. 5.

[2] Ibidem, s. 16.

[3] http://www.bankomaty.org.pl/77, [5.11.2014 r.].

[4] *Przestępczość z Wykorzystaniem Elektronicznych Instrumentów Płatniczych*, J. Kosiński red., Szczytno 2003, s. 9.

Do 1991 roku, karty płatnicze nie były powszechnie dostępne, przynajmniej oficjalnie, dla Polaków. Nie oznacza to, że nie były znane i akceptowane. Powołany w Polskim Biurze Podróży ORBIS Dział Legitymacji Kart był pierwszym polskim centrum autoryzacyjnym posiadającym umowy na akceptację kart w hotelach, sieciach sklepów (Pewex, Baltona, Cepelia), galeriach sztuki oraz najwyższej kategorii restauracjach[5].

Obecnie na kartach bankomatowych poprzez mechaniczny, silny nacisk na podłoże, wytłacza się podstawowe informacje, takie, jak:

- numer karty – jest to ściśle określony układ cyfr, pierwsze cyfry stałe, np. VISA – 4xxx xxxx xxxx xxxx lub 4xxx xxx xxx xxx, EUROCARD/MasterCard – 5xxx xxxx xxxx xxxx czy Diners Club 3xxx xxx xxx xxxx (30,36,38),
- nazwisko i imię posiadacza karty,
- data ważności – od kiedy i do kiedy karta jest ważna,
- mogą również być umieszczone inne dane – kod terytorialny kraju, rok, od którego posiadacz należy do danej organizacji, itp.[6]

Na czołowej stronie karty (awersie) znajdują się także następujące elementy:

- nazwa i symbol banku lub organizacji, która kartę wystawiła,
- symbol (znak firmowy) systemu, w ramach którego karta została wystawiona (np. symbol VISA),
- hologram,
- mikroprocesor (w przypadku kart mikroprocesorowych).

Na tylnej stronie karty (rewersie) jest umieszczany:

- pasek magnetyczny zawierający zakodowane dane dotyczące karty,
- pasek na podpis, gdzie posiadacz karty zobowiązany jest podpisać się w chwili odbioru karty i inne[7].

---

[5] *Przestępczość z wykorzystaniem kart płatniczych*, M. Zajder, J. Kosiński (red.), Szczytno 2001, s. 74.

[6] *Przestępczość z wykorzystaniem kart płatniczych*, M. Zajder, J. Kosiński (red.), Szczytno, 2001, s. 136.

[7] R. Łuczak, M. Wojtas, K. Woźniak, *Przestępstwa związane z obrotem kartami płatniczymi*, POLCARD CO. Ltd, s. 6.

Większość kart jest również zabezpieczona za pomocą reliefowych hologramów tęczowych. Choć zazwyczaj nie są one wysokiej klasy, to jednak można uznać, że są w miarę dobrym zabezpieczeniem[8].

Obecnie w Polsce banki wydają najwięcej kart płatniczych zabezpieczonych tzw. chipem i paskiem magnetycznym, wprowadzonym na początku lat 70-tych, umieszczonym na rewersie karty. Dane zapisane na pasku są kodowane na trzech ścieżkach:

- pierwsza – alfanumeryczna zawiera 76 znaków,
- druga – numeryczna, zawiera 37 znaków,
- trzecia – numeryczna, zawiera 105 znaków,

Pasek magnetyczny na każdej z opisanych ścieżek zawiera informacje, takie, jak:

- dane o posiadaczu karty (imię, nazwisko, czasami inicjał nazwiska i imienia),
- numer karty,
- datę ważności,
- szyfrowaną informację, np. cyfrę kontrolną oraz określenie rodzaju karty,
- kod usługi – trzycyfrowy kod określający zakres dopuszczalnej wymiany (krajowa, zagraniczna, lokalna) oraz czy inne urządzenia odczytu są dostępne dla danej karty.

Skimming to przestępstwo polegające na nielegalnym skopiowaniu zawartości paska magnetycznego karty płatniczej bez wiedzy jej posiadacza, w celu wytworzenia kopii a następnie wykonywania nieuprawnionych płatności za towary i usługi lub wypłat z bankomatów. Obecnie skimming jest wymierzony także w karty z paskiem magnetycznym oraz wbudowanym mikroprocesorem z układami niechronionej klasy SDA, czyli *Static Data Authentication*[9] (statyczne uwierzytelnianie danych) oraz DDA, co oznacza *Dynamic Data Authentication*[10] (dynamiczne uwierzytelnianie danych).

---

[8] *Przestępczość z wykorzystaniem kart płatniczych*, M. Zajder, J. Kosiński (red.), Szczytno, 2001, s. 136.

[9] http://zbp.pl/public/repozytorium/dla_bankow/rady_i_komitety/technologie_bankowe/publikacje/Migracja_na_standard_EMV_aspekty_organizacyjno_-_techniczne.pdf, [10.01.2016].

[10] Ibidem.

SDA jest najprostszą metodą uwierzytelnienia karty, która pozwala nie tyle uwierzytelnić samą kartę, co raczej dane zapisane na karcie. Cel ten jest realizowany poprzez wpisanie przez wydawcę karty istotnych danych na karcie, przy użyciu prywatnego klucza wydawcy karty. Wyliczony w ten sposób podpis jest umieszczony na karcie. Wraz z podpisem na karcie znajduje się klucz publiczny wydawcy karty w formie certyfikatu. Certyfikat taki wystawia organizacja płatnicza, której logo będzie na karcie[11]. Ma to na celu, przede wszystkim, sprawdzenie czy nie wystąpiła nieautoryzowana zmiana wartości ważnych dla bezpieczeństwa systemu płatniczego parametrów zapisanych na karcie w trakcie jej personalizacji[12].

DDA zapewnia i potwierdza autentyczność danych znajdujących się na karcie oraz danych wygenerowanych przez kartę i danych otrzymanych z terminala w trakcie transakcji EMV (skrót od Europay, MasterCard, Visa). Jest to specyfikacja techniczna kart mikroprocesorowych, powstała na mocy porozumienia organizacji płatniczych, ujednolicająca wymagania tych organizacji odnośnie karty z mikroprocesorem[13], która uchodzi za bezpieczniejszą[14]. W tym przypadku jest kopiowana jedynie zawartość paska magnetycznego. Ponieważ skopiowana karta w elektronicznych systemach bankowych zachowuje się jak karta oryginalna, wszystkie operacje wykonane za jej pomocą odbywają się kosztem posiadacza oryginalnej karty i obciążają jego rachunek.

Skimming bankomatowy

W celu pozyskiwania danych z paska magnetycznego przestępcy instalują na bankomatach lub w ich wnętrzu (czytniku) specjalne urządzenia, tzw. skimmery. Instalują także urządzenia

[11] Ibidem.

[12] http://zbp.pl/public/repozytorium/dla_bankow/rady_i_komitety/technologie_bankowe/publikacje/Migracja_na_s tandard_EMV_aspekty_ organizacyjno_-_techniczne.pdf, [11.03.2015].

[13] https://www.polcard.pl/content/polcard/strona-glowna/slowniczek.html [10.01.2016].

[14] http://zbp.pl/public/repozytorium/dla_bankow/rady_i_komitety/technologie_bankowe/publikacje/Migracja_na_s tandard_EMV_aspekty_organizacyjno_-_techniczne.pdf, [11.03.2015].

przechwytujące sekwencje cyfr tworzące numer PIN (Personal Identification Number), czyli osobisty numer identyfikacyjny, zwykle 4-cyfrowy, służący do potwierdzania transakcji dokonywanych w bankomatach oraz w terminalach płatniczych dzięki umieszczonej tam kamerze, przerobionej klawiaturze lub układowi elektronicznemu umieszczonemu w czytniku na kartę. PIN jest elektronicznym odpowiednikiem podpisu złożonego na potwierdzeniu transakcji. Zarejestrowane w ten sposób informacje są najczęściej transmitowane drogą radiową. Umieszcza się je na fałszywych kartach, tzw. białych plastikach, za pomocą których możliwe jest pobieranie gotówki z kont klientów banków za pośrednictwem bankomatów[15].

Największymi producentami bankomatów są firmy: NCR, Wincor Nixdorf oraz Diebold[16]. Według szacunków ATM Industry Association, w 2008 roku na świecie działało ponad 1,7 mln urządzeń tego typu. Liczba bankomatów operatorów bankowych stanowi 69,74% całkowitej liczby bankomatów w Polsce. Bankomaty operatorów niebankowych stanowią 30,26% tej liczby, z czego 23,16% to bankomaty Euronet. Wśród bankowych operatorów prym wiedzie PKO Bank Polski SA z 2978 bankomatami co stanowi 23%, za nim z 17% udziałem znajduje się Bank Polskiej Spółdzielczości SA (2223 bankomatów), następnie Bank Pekao SA z 14% udziałem (1833 bankomatów) w rynku operatorów bankowych. Trzy wyżej wymienione banki stanowią ponad połowę (54%) wszystkich bankomatów operatorów bankowych.

Rynek niebankowych operatorów bankomatów zdominowany został przez firmę Euronet Polska Sp. z o.o. z udziałem 76%. Bankomaty SKOK 24 (8%), eCards SA (6%) oraz Global Cash (2%) należą do Towarzystwa Finansowego SKOK SA zajmując łącznie 16% rynku. Trzecią siłą na tym rynku jest Planet Cash4You Sp. z o.o. z 8% udziałem w rynku[17].

Bankomaty są przedmiotem działalności przestępczej. Między innymi za ich pośrednictwem, przy zamontowaniu specjalnych urządzeń, przestępcy kopiują karty bankomatowe, a następnie

[15] http://www.knf.gov.pl/Images/Bezp_finansowe_tcm75-39005.pdf, [23.02.2015].

[16] http://mfiles.pl/pl/index.php/Bankomat, [6.11.2014].

[17] https://www.nbp.pl/systemplatniczy/bankomaty/bankomaty.pdf, [04.02.2016].

przy użyciu tych danych dokonują nieautoryzowanych, bez zgody i zezwolenia dysponenta karty, wypłat środków pieniężnych z kont klientów banku.

Tabela 1. Liczba bankomatów w latach 2010-2014, według danych NBP[18]

Lp.	Rok	Liczba bankomatów	Liczba transakcji	Ogólna wartość transakcji w zł
1	2014	20 531	770 838 756	307 276 925 754
2	2013	18 876	778 005 072	297 286 491 084
3	2012	18 188	746 738 629	285 087 727 626
4	2011	17 392	707 306 789	270 928 793 491
5	2010	16 413	672 270 122	252 836 278 647

Tabela 2. Liczba incydentów w Banku PEKAO SA w latach 2010-2015, według danych Banku PEKAO SA[19]

Lp.	Rok	Liczba incydentów	Liczba skopiowanych kart bankomatowych
1	2015	249	11 412
2	2014	183	6 143
3	2013	134	7 241
4	2012	136	5 068
5	2011	71	3 089
6	2010	38	663

Jak wynika z powyższych danych, problem skimmingu z roku na rok narasta. W samym tylko Banku PEKAO SA zarówno liczba incydentów, jak również liczba skopiowanych kart zwiększa się z każdym rokiem powodując duże straty różnych banków, ponieważ jedna nakładka umieszczona na bankomacie kopiuje

[18] http://www.nbp.pl/home.aspx?f=/systemplatniczy/karty_platnicze.html, [06.01.2015].

[19] Dane uzyskane od pracownika Banku PEKAO S.A., materiały własne.

karty bankomatowe różnych banków. Mimo, iż bankomat jest zainstalowany przez jeden bank, to korzystają z niego klienci różnych banków i wszystkie te karty są kopiowane w czasie, gdy nakładka jest zamontowana. Bank PEKAO S.A. podaje, że nakładki najczęściej były montowane na bankomaty typu Wincor i NCR. W latach od 2010 do 2013 w statystyce kopiowań dominowały bankomaty typu Wincor bez względu na typ, w 2014 r. mniej więcej tyle samo kopiowań było na bankomatach typu Wincor i NCR, natomiast w roku 2015 ponownie przeważały Wincory. Pomimo zdecydowanej przewagi kopiowań na bankomatach typu Wincor, zdarzały się niejednokrotnie kopiowania na bankomatach typu NCR. W innych typach bankomatów skimmingu nie stwierdzono.

Ponieważ proceder skimmingu jest przestępstwem, tak banki, jak i instytucje porządku publicznego starają się mu zapobiegać i eliminować go. Banki i organy ścigania ściśle współpracują ze sobą, w celu zwalczania problemu. W Policji powstają specjalne komórki złożone, których zadaniem jest wykrywanie i zwalczanie skimmingu. Policjanci, realizują proces wykrywczy a przedstawiciele banków, wytypowani do kontaktów, udzielają pomocy organom ścigania. Formą zwalczania procederu skimmingu jest także *Forum przeciwdziałania przestępczości z użyciem kart płatniczych*. Jest to struktura ekspercka powołana przez banki, działająca w ramach Rady Wydawców Kart Bankowych Związku Banków Polskich[20].

Banki prowadzą również tak zwaną *politykę ryzyka*, polegającą na tworzeniu struktury organizacyjnej np. komisji, w której skład wchodzą ogniwa odpowiedzialne za systemy bezpiecznego obrotu kartami płatniczymi, wychwytywanie, zapobieganie i wykrywanie m.in. skimmingu. Komisja taka wydaje rekomendacje ostrożnościowe dla bezpieczeństwa w zakresie zarządzania ryzykiem operacyjnym oraz ryzykiem systemów informatycznych[21].

Istotne jest również oddziaływanie prewencyjne banków poprzez tworzenie procedur bezpieczeństwa. Banki monitorują

[20] R. Kaszubski, Ł. Obzejta, *Karty płatnicze w Polsce*, Warszawa 2012, s. 398.

[21] G. Szwajkowska, P. Kwaśniewski, K. Leżoń, F. Woźniczka, *Usługi bankowości elektronicznej dla klientów detalicznych, charakterystyka i zagrożenia*, Urząd Komisji Nadzoru Finansowego, Warszawa 2010, s. 15.

transakcje dokonywane przez swoich klientów, analizują zachowania klienta dotyczące dokonywanych płatności. Nietypowe płatności są weryfikowane za pomocą zdefiniowanych w systemie warunków logicznych, w celu zidentyfikowania transakcji nieuprawnionych (oszukańczych). Wygenerowany alert jest weryfikowany przez operatora, który może podjąć określone działania, np. kontaktuje się z posiadaczem karty[22].

Banki nieustannie dostosowują i zabezpieczają systemy informatyczne obsługujące transakcje za pomocą kart płatniczych. Karty płatnicze dzieli się na:

- karty z paskiem magnetycznym – nośnikiem informacji jest pasek magnetyczny, na którym są zapisane informacje pozwalające na dokonanie transakcji (numer karty, data ważności itd.). Na karcie tego typu nie jest zapisywany numer PIN, służący do uwierzytelnienia transakcji,
- karty z układem elektronicznym (karty chipowe, mikroprocesorowe) – dane niezbędne do autoryzacji transakcji są zapisane w mikroprocesorze umieszczonym w karcie. Standard obsługi takich transakcji jest opracowany przez organizację zrzeszającą największych wydawców kart płatniczych: Europay, Mastercard i Visa (EMV), stąd karty chipowe, mają opinię zgodnych ze standardem EMV[23].

Podział ten ma duże znaczenie praktyczne z uwagi na możliwości identyfikacji użytkownika karty za pomocą paska magnetycznego i mikroprocesora i wpływ tych informacji na wypłatę środków pieniężnych z kont bankowych. EMV jest to międzynarodowy standard odpowiadający za autoryzację płatności kartowych poprzez kombinację mikroprocesor + kod pin. Pomimo stosowania norm EMV zdarzają się sytuacje, że podczas wypłacania fałszywą kartą, zawierającą dane skopiowane podczas skimmingu, system zezwala na wypłatę gotówki na podstawie identyfikacji danych tylko z paska magnetycznego, zakładając, iż mogło nastąpić np. uszkodzenie mikroprocesora bądź inna przeszkoda, która chwilowo wyeliminowała identyfikację karty poprzez dane

[22] G. Szwajkowska, P. Kwaśniewski, K. Leżoń, F. Woźniczka, *Usługi bankowości elektronicznej dla klientów detalicznych, charakterystyka i zagrożenia*, Warszawa 2010, s. 18.

[23] Witryna NBP.

zawarte w mikroprocesorze. Jeżeli jednak takie wypłaty gotówki powtarzają się, system blokuje możliwość wypłaty. Zatem normy EMV, co prawda, nie zwiększają trudności w kopiowaniu paska magnetycznego, ale chronią gotówkę przed nieautoryzowanymi wypłatami. Według szacunków Komisji Nadzoru Finansowego na koniec 2009 r. ponad 25% bankomatów w Polsce nie było zgodnych z EMV (tzn. że odczytywały one dane jedynie z paska magnetycznego)[24].

W tej sytuacji pewna, niemała zresztą, liczba bankomatów niezgodnych z systemem EMV umożliwiała międzynarodowym gangom wykorzystywanie tych urządzeń do wybierania gotówki za pomocą białych plastików bądź innych kart zawierających dane skopiowane z pasków magnetycznych. Za taki stan odpowiada strona, która nie była dostosowana do EMV, czyli bank jako właściciel bankomatu.

Zadaniem analizy dwóch spraw prowadzonych przez funkcjonariuszy Komendy Wojewódzkiej Policji w Olsztynie, jest ustalenie sposobu działania zorganizowanych grup przestępczych specjalizujących się w skimmingu. Terenem działania obu grup była tzw. wschodnia ściana Polski – Olsztyn oraz Białystok i jego okolice.

Przykład Nr 1: grupa bułgarska

W lutym 2012 r., Prokuratura Okręgowa w Olsztynie przekazała do Wydziału Walki z Przestępczością Gospodarczą Komendy Wojewódzkiej Policji w Olsztynie do prowadzenia sprawę dotyczącą skimmingu, popełnionego w bankomacie znajdującym się przy jednej z ulic Olsztyna. Do Komendy Miejskiej Policji w Olsztynie zgłosiły się osoby pokrzywdzone, zawiadamiając, iż z ich rachunków bankowych zostały wyprowadzone pieniądze. Wypłaty były dokonywane w bankomatach w Bułgarii. Wpłynęło też zawiadomienie o popełnieniu przestępstwa z banków, w których znajdowały się rachunki pokrzywdzonych osób. Banki, w ramach reklamacji, zwróciły pieniądze klientom i tym samym weszły w rolę

[24] G. Szwajkowska, P. Kwaśniewski, K. Leżoń, F. Woźniczka, *Usługi bankowości elektronicznej dla klientów detalicznych, charakterystyka i zagrożenia*, Warszawa 2010, s. 20.

pokrzywdzonych. Na pismo policjantów z prośbą o przekazanie zapisu monitoringu bankomatu, w którym nastąpił skimming, Departament Bezpieczeństwa PKO BP w Olsztynie poinformował, iż materiał wizyjny z monitoringu przedmiotowego bankomatu nie zachował się z uwagi na przekroczony czas archiwizacji.

W listopadzie 2011 r. mieszkaniec Olsztyna, dokonując transakcji przy użyciu karty w bankomacie objętym szczególnym nadzorem policjantów i pracowników jednego z pokrzywdzonych banków zauważył, że w bankomacie są zamontowane dwie nakładki skimmujące. O fakcie tym powiadomił Policję. Tego samego dnia przyjęto od niego protokół zawiadomienia o popełnieniu przestępstwa, równocześnie dokonując przesłuchania w charakterze świadka. Szczegółowym oględzinom poddano wskazany bankomat, zabezpieczono nakładki, przekazując je dalej do badania w ramach ekspertyzy kryminalistycznej.

Powiadomiony o zaistniałym zdarzeniu pracownik właściciela bankomatu, wskazany do współpracy z organami ścigania niezwłocznie złożył zawiadomienie o popełnieniu przestępstwa oraz wniosek o ściganie karne jednocześnie przekazując płytę CD z zapisem monitoringu. Dalej udało się ustalić, że dwaj mężczyźni podejrzewani o założenie nakładek skimmujących na opisywanym bankomacie byli zakwaterowani w jednym z hoteli znajdujących się w centrum Olsztyna. Mężczyźni zostali rozpoznani przez świadków, co pozwoliło uzyskać ich pełne dane osobowe. Posiadając takie informacje, policjanci podjęli intensywne poszukiwania podejrzewanych osób na skalę międzynarodową.

Biegły, wydając opinię na temat nakładek skimmujących zdjętych z bankomatu, stwierdził, iż urządzenia te służyły do pozyskiwania numerów kart płatniczych oraz kodów PIN tych kart. Poza tym po przekodowaniu nieczytelnych zapisów na nośnikach pamięci umieszczonych na nakładkach, biegły odczytał w całości zapis 162 kart płatniczych, z tego ze 152 kart udało się odczytać 16 cyfrowy numer nadrukowany na powierzchni karty płatniczej. W odczytanych zapisach nie było danych właścicieli kart bankomatowych. We wnioskach końcowych biegły napisał, iż „w efekcie odczytania zawartości skimmera i kamery oszuści byli w stanie w prosty sposób wyprodukować karty pozwalające na wybieranie

pieniędzy z bankomatów za pomocą poprawnych kodów PIN bez wiedzy właściciela karty”[25].

Przesłuchany w charakterze świadka pracownik pokrzywdzonego banku potwierdził, iż właścicielem skopiowanych kart bankomatowych jest jego bank. Roszczenia klientów z tytułu skimmingu zostały w całości uznane przez bank. Bank poniósł stratę z tytułu skopiowania kart w kwocie 59.417,59 zł. Ta kwota wynikała jedynie z wypłat gotówki ze skopiowanych kart w bankomatach nie współpracujących z systemem EMV.

Pod koniec marca 2012 r. policjanci uzyskali informację, iż na terenie Starego Miasta w Olsztynie widziano poszukiwanych mężczyzn, którzy są prawdopodobnie narodowości bułgarskiej lub rumuńskiej. Podjęto obserwację i ustalono, że mężczyźni ci udali się pociągiem do Elbląga, gdzie w jednym z hoteli wynajęli pokój. W recepcji uzyskano dane tych osób, które zgadzały się z danymi poszukiwanych mężczyzn. Zdecydowano zatrzymać mężczyzn jako sprawców zamontowania nakładek skimmujących na bankomat w Olsztynie. Ponieważ były to osoby narodowości bułgarskiej, czynności przeprowadzano z udziałem tłumacza języka bułgarskiego. Dokonano przeszukania zatrzymanych osób, ujawniając: telefony komórkowe z kartami pamięci i karty płatnicze. Pieniądze, znalezione u podejrzanych, tytułem tymczasowego zajęcia mienia ruchomego zostały zabezpieczone. Natomiast w wyniku przeszukania pokoju hotelowego w Elblągu, który wynajęli podejrzani znaleziono: netbooki, plastikowy element (osłona wrzutnika kart) z baterią, płytką elektroniczną z podzespołami i głowicą magnetyczną, połączone kablami, element plastikowy koloru szarego z zielonym okienkiem, (osłona podajnika pieniędzy-banknotów) z zamontowanymi na odwrocie dwiema bateriami NOKIA BL-5C, płytką elektroniczną z podzespołami i gniazdem USB 2,0 i kamerą, połączone kablami, telefony komórkowe marki NOKIA 1208 z wlutowanymi w tylną część obudowy kablami i wtyczkami, kable USB 2,0, rolki taśmy dwustronnej przylepnej. O zatrzymaniu mężczyzn powiadomiono Konsulat Republiki Bułgarii we Wrocławiu. Prokurator nadzorujący śledztwo przedstawił mężczyznom zarzuty i wniósł do sądu

[25] J. Biskupski, *Ekspertyza kart magnetycznych płatniczych nr 05/14*, materiały własne KWP Olsztyn.

wniosek o zastosowanie w stosunku do nich środka zapobiegawczego w postaci tymczasowego aresztowania.

W toku dalszego postępowania okazało się, że mężczyźni popełnili przestępstwo skimmingu w okresie od września 2011 r. do marca 2012 r. na terenie Olsztyna i Elbląga. Obaj przyznali się do dokonania zarzucanych im czynów i złożyli obszerne wyjaśnienia. W trakcie przesłuchań ustalono, iż zatrzymani dwaj obywatele narodowości bułgarskiej byli jedną z kilku grup „skimmujących" na terenie Polski. Członkowie tych grup wymieniali się nakładkami, które po dokonaniu nielegalnych kopiowań zdejmowali z bankomatów i umieszczali w skrytce. Skrytką było miejsce w suficie wykonanym z kasetonów w korytarzu jednego z warszawskich hoteli. Jeden z kasetonów łatwo dawał się wyjąć, co umożliwiało położenie skimmera na innych kasetonach. W toku postępowania zebrano obszerny materiał dowodowy, który potwierdzał popełnienie skimmingu przez podejrzanych. Sprawa zakończyła się wyrokiem skazującym dla oskarżonych mężczyzn narodowości bułgarskiej.

Ze sprawy zostały wyłączone materiały do odrębnego postępowania przeciwko osobie, która nadzorowała i koordynowała przestępcze działania skazanych osób. W wyłączonym postępowaniu wystosowano Europejski Nakaz Aresztowania i na jego mocy po kilku miesiącach dokonano zatrzymania osoby kierującej całą grupą, w momencie gdy wybrała się na wakacje do Grecji. Również w tym przypadku całe postępowanie zakończyło się prawomocnym wyrokiem pozbawienia wolności.

Przykład Nr 2: grupa łotewska

W okresie od maja 2013 r. do listopada 2013 r. na terenie Giżycka, Białegostoku, Bielska Podlaskiego, Radzynia Podlaskiego, Siedlec, Pisza, Łukowa, Puław, Lublina i innych miejscowości w Polsce ujawniono fakty kopiowania danych z kart bankomatowych. Ich efektem były nieautoryzowane wypłaty w bankomatach na terenie Tajlandii, USA i innych państw. Prokuratura Rejonowa w Giżycku wszczęła śledztwo, do którego dołączono postępowania karne dotyczące kopiowania kart w innych miejscowościach na terenie Polski.

W związku ze śledztwem, w listopadzie 2013 r. na terenie Giżycka zatrzymano czterech obywateli Republiki Łotwy, którzy na bankomatach w tym mieście zakładali urządzenia służące do kopiowania pasków magnetycznych kart bankomatowych. W grudniu 2013 r. śledztwo w całości powierzono Wydziałowi do Walki z Przestępczością Gospodarczą Komendy Wojewódzkiej Policji w Olsztynie. Ustalono, iż na początku maja 2013 r. obywatel Republiki Łotwy zorganizował grupę przestępczą, w skład której wchodzili obywatele Łotwy. Grupą kierował również Łotysz. Celem grupy było popełnianie na terenie Polski przestępstw polegających na nielegalnym kopiowaniu danych z pasków magnetycznych kart bankomatowych, nielegalne pozyskiwanie kodów PIN tychże kart i wytwarzanie duplikatów takich kart. Następnie na terenie Tajlandii, USA i innych państw, były realizowane wypłaty środków płatniczych z rachunków bankowych. Aby zrealizować przestępczy cel, zatrzymani mężczyźni, od kierującego grupą, otrzymali urządzenia służące do kopiowania danych z kart bankomatowych, czyli tzw. nakładki na czytnik kart bankomatowych oraz kamery, za pomocą których rejestrowano kody PIN kart bankomatowych używanych w bankomacie. Rolą zatrzymanych mężczyzn, w tej grupie, było zakładanie w bankomatach położonych na terenie Polski nakładek, które kopiowały dane pasków magnetycznych użytych w czytniku kart bankomatowych oraz kamer, które rejestrowały kody PIN takich kart. Pozyskane w ten sposób kody PIN mężczyźni dopasowywali do skopiowanych kart bankomatowych. Pozyskane dane tj. skopiowane paski magnetyczne kart bankomatowych i przypisane takim kartom kody PIN bezpośrednio po ich uzyskaniu były przesyłane elektronicznie do przywódcy grupy. Ten przekazywał je nieustalonej w śledztwie osobie, najprawdopodobniej obywatelowi Bułgarii. Przy wykorzystaniu pozyskanych danych skopiowanych kart sporządzano, w nieustalonych w śledztwie okolicznościach, fałszywe karty bankomatowe. Przy użyciu fałszywych kart płatniczych oraz pozyskanych kodów PIN, nieustalone w śledztwie osoby dokonywały wypłat środków pieniężnych na terenie innych państw, głównie Tajlandii i USA. Część tych pieniędzy była przekazywana przez dowodzącego grupą przestępczą zaufanemu człowiekowi, zatrzymanemu w Giżycku. Ten z kolei dzielił je pomiędzy siebie

i pozostałych sprawców. Już w trakcie prowadzenia przestępczego procederu na terenie Polski „przywódca" przekazał wyznaczonemu człowiekowi adres elektroniczny do wspomnianego „Bułgara", do którego należało wysyłać pozyskane w Polsce dane skopiowanych kart i kody PIN.

W połowie listopada 2013 r. dwaj z zatrzymanych mężczyzn, zaproponowali udział w tej przestępczej działalności na terenie Polski, dwóm obywatelom Republiki Łotwy, którzy zostali zatrzymani wraz z nimi. „Nowi" po wyrażeniu zgody na udział w przestępstwie, podjęli się zakładania i zdejmowania nakładek z bankomatów oraz prowadzenia obserwacji okolicy bankomatu w czasie, gdy nakładki są montowane oraz później w czasie ich pracy. Wymienieni mieli ostrzegać pozostałych sprawców, gdyby doszło do ujawnienia przez postronne osoby faktu zamontowania nakładek. Mężczyźni zostali przeszkoleni w zakładaniu i zdejmowaniu nakładek. Zgodnie z poczynionymi uzgodnieniami mieli oni otrzymywać procent z kwot uzyskanych w wyniku przestępczej działalności. W listopadzie 2013 r. za pośrednictwem portalu internetowego dokonana została rezerwacja mieszkania w Giżycku dla 4 osób. Przyjechali do Polski wynajętym samochodem. Na miejsce dotarli w godzinach wieczornych i zatrzymali się w wynajętym mieszkaniu. W czasie pobytu w Polsce czterej mężczyźni kilkakrotnie montowali i zdejmowali nakładki na bankomatach należących do różnych banków.

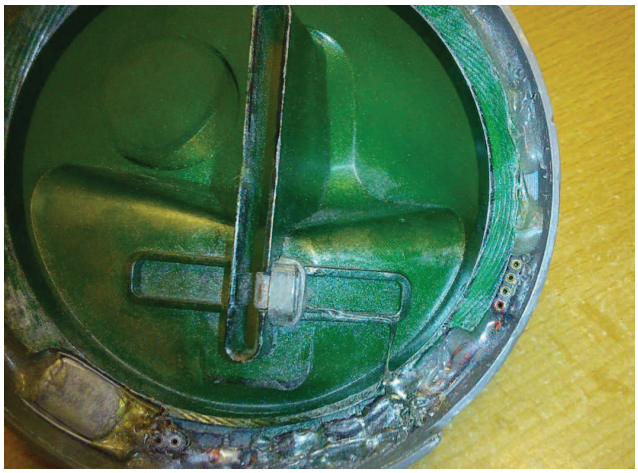
Przed budynkiem mieszkalnym, w którym mężczyźni wynajmowali mieszkanie, zabezpieczono samochód, którym przyjechali. W toku przeszukania wynajętego mieszkania w Giżycku oraz samochodu, ujawniono i zabezpieczono między innymi 4 urządzenia elektroniczne służące do kopiowania danych z kart płatniczych (tzw. nakładki), laptop, tablet i zewnętrzne dyski pamięci. Na zabezpieczonych u sprawców nośnikach pamięci biegły z zakresu informatyki ujawnił kilka tysięcy plików zawierających zdjęcia klawiatur bankomatów oraz osób przebywających w okolicy bankomatów.

W zabezpieczonej nawigacji samochodowej biegły ustalił wprowadzane do tego urządzenia trasy do punktów, które były celem zatrzymanych. Analiza nazw wprowadzanych do pamięci nawigacji wykazała, iż osoba(y) posługujące się tą nawigacją,

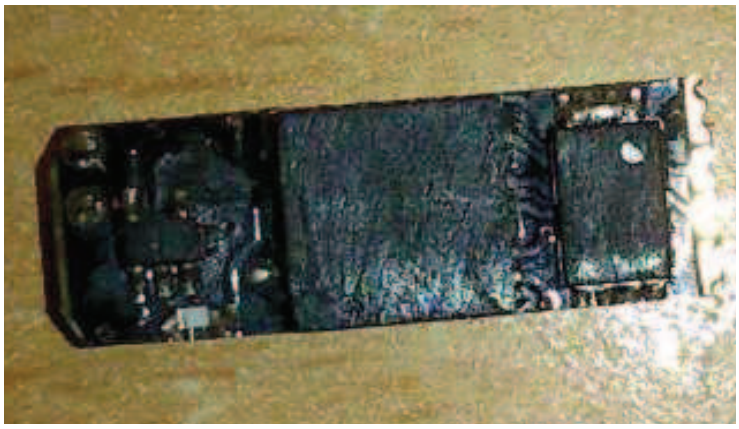
4 krotnie przyjeżdżały do Polski, po czym wracały na Łotwę. Istniała przy tym korelacja wprowadzanych nazw polskich miejscowości z miejscowościami, w których sprawcy montowali nakładki i kamery w bankomatach.

Powołany w sprawie biegły poddał badaniom zabezpieczone u sprawców urządzenia elektroniczne w postaci nakładek na bankomat.

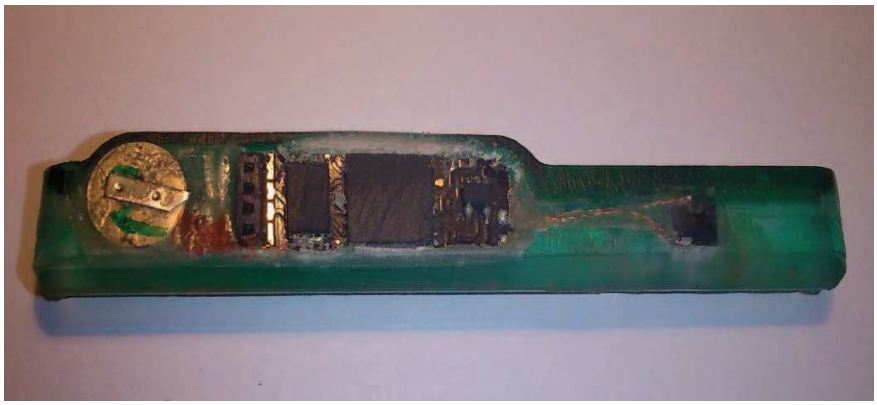
Rycina 1. Skimer SK 0
Źródło: J. Biskupski, *Ekspertyza kart magnetycznych płatniczych nr 05/14*, materiały własne KWP Olsztyn.



Rycina 2. Skimer 30
Źródło: J. Biskupski, *Ekspertyza kart magnetycznych płatniczych nr 05/14*, materiały własne KWP Olsztyn.



Rycina 3. Skimmer typ 2 – montowany w szczelinie
Źródło: J. Biskupski, *Ekspertyza kart magnetycznych płatniczych nr 05/14*, materiały własne KWP Olsztyn.



Rycina 4. Skimmer typ 2 - montowany w szczelinie
Źródło: J. Biskupski, *Ekspertyza kart magnetycznych płatniczych nr 05/14*, materiały własne KWP Olsztyn.

W opinii końcowej biegły stwierdził, że „przekazane do badań urządzenia służyły do pozyskiwanie numerów kart płatniczych oraz kodów PIN kart osób, które korzystały z bankomatu, na którym mogły być one założone jako dodatkowe atrapy. Atrapy dobrane kolorem i wzornictwem miały maskować ukryte w nich przedmiotowe właściwe urządzenia [...] urządzenie te nie są wyposażeniem bankomatów, posiadają własne niezależne zasilania oraz są jedynie dopasowane kształtem i kolorem do bankomatów”[26]. W badanych urządzeniach biegły odnalazł półprzewodnikowe pamięci nieulotne, które pozwalają na zapis danych elek-

[26] J. Biskupski, *Ekspertyza kart magnetycznych płatniczych nr 05/14*, materiały własne KWP Olsztyn.

tronicznych. W wyniku zdekodowania ich zawartości otrzymano numery kart płatniczych, które zostały przez te urządzenia odczytane. W urządzeniach służących do nagrywania kodów PIN biegły ujawnił filmy video zawierające obrazy klawiatury bankomatu.

Wobec zatrzymanych mężczyzn został zastosowany środek zapobiegawczy w postaci tymczasowego aresztowania. W toku śledztwa ustalono elektroniczne skrzynki pocztowe, na które jeden z zatrzymanych wysyłał dane zawierające skopiowane paski magnetyczne kart, w celu umieszczenia ich na fałszywych kartach płatniczych, oraz numery PIN.

Mężczyźni, przesłuchani w charakterze podejrzanych przyznali się do popełnienia zarzucanych im przestępstw i złożyli szczegółowe wyjaśnienia. Zostali skazani prawomocnym wyrokiem Sądu za udział w grupie przestępczej i skimming bankomatowy. Pozostali, są objęci poszukiwaniem za pomocą Europejskiego Nakazu Aresztowania.

Zakończenie

Przedstawione przykłady pozwalają na nakreślenie *modus operandi* sprawców skimmingu bankomatowego. Przede wszystkim przestępstwo jest popełniane w sposób zorganizowany przez kilka osób. Grupa ma przywódcę, a pozostali tworzą zespoły 2 – 4 osobowe. Każdy z małych zespołów również jest kierowany jednoosobowo. Czasem kilka zespołów, należących do jednej grupy, pracuje równolegle w różnych mniejszych miastach lub częściach dużej aglomeracji. Rytm pracy zespołu jest następujący: zespół instaluje nakładki na bankomaty, a po pewnym czasie je deinstaluje, wymienia nakładki na inne z innym zespołem używając skrytki w ogólnie dostępnym miejscu, i znowu instaluje nakładki. Zadaniem zespołu jest także obserwacja bankomatu, w czasie gdy ma zainstalowane nakładki skimmujące. Cykl się powtarza, przy czym kierujący zespołem dane, uzyskane ze skimmingu, przekazuje elektronicznie osobie zajmującej się wytwarzaniem fałszywych kart bankomatowych. Wyprodukowane karty bankomatowe i dopasowane do nich PIN-y są przesyłane innemu ze-

społowi działającemu czasem na terenie innego państwa, i tam dochodzi do wypłat gotówkowych z bankomatów. Zespoły lub poszczególni członkowie grupy specjalizują się w określonych czynnościach jak, montowanie skimmerów, wypłata z użyciem fałszywej karty, wytwarzanie fałszywych kart płatniczych. Przestępczy dochód trafia do przywódcy całej grupy zorganizowanej, który rozdziela zysk między zespoły i indywidualnych wykonawców.

W ustaleniach wykrywczych istotną rolę odegrała kryminalistyczna ekspertyza magnetycznych kart płatniczych i urządzeń montowanych w szczelinach bankomatowych. Opinia biegłego jednoznacznie wskazała cel montowania takich urządzeń na bankomatach przez osoby do takich działań nieuprawnione.

Sprawcy skimmingu doskonalą swoje urządzenia i najchętniej działają w miejscowościach turystycznych lub na gęsto zaludnionych obszarach. Problem skimmingu istnieje i jak wskazują statystyki powiększa się, chociaż powstają nowe pomysły „wyciągnięcia pieniędzy z bankomatów".

Bibliografia

1. http://mfiles.pl/pl/index.php/Bankomat, [6.11.2014].
2. http://www.knf.gov.pl/Images/Bezp_finansowe_tcm75-39005.pdf, [23.02.2015].
3. http://www.nbp.pl/home.aspx?f=/systemplatniczy/karty_platnicze.html, [06.01.2015].
4. http://zbp.pl/public/repozytorium/dla_bankow/rady_i_komitety/technologie_bankowe/publikacje/Migracja_na_standard_EMV_aspekty_organizacyjno_-_techniczne.pdf, [10.01.2016].
5. https://www.nbp.pl/systemplatniczy/bankomaty/bankomaty.pdf, [04.02.2016].
6. https://www.polcard.pl/content/polcard/strona-glowna/ slowniczek.html, [10.01.2016].
7. http://www.bankomaty.org.pl/77 [5.11.2014 r.].
8. Biskupski J., *Ekspertyza kart magnetycznych płatniczych nr 05/14*, materiały własne KWP Olsztyn.
9. Kaszubski R., Obzejta Ł., *Karty płatnicze w Polsce*, Warszawa 2012.
10. Kosiński J., *Przestępczość z Wykorzystaniem Elektronicznych Instrumentów Płatniczych*, Szczytno 2003.

11. Łuczak R., Wojtas M., Woźniak K., *Przestępstwa związane z obrotem kartami płatniczymi*, POLCARD CO. Ltd.
12. Szwajkowska G., Kwaśniewski P., Leżoń K., Woźniczka F., *Usługi bankowości elektronicznej dla klientów detalicznych, charakterystyka i zagrożenia*, Urząd Komisji Nadzoru Finansowego, Warszawa 2010.
13. Witryna NBP.
14. Zajder M., Kosiński J. (red.), *Przestępczość z wykorzystaniem kart płatniczych*, Szczytno 2001.