Bezpieczny Bank
1(62)/2016

Paweł Opitek*

WPŁYW STANDARDU EMV NA NIELEGALNE DZIAŁANIA Z WYKORZYSTANIEM KART PŁATNICZYCH W KONTEKŚCIE PRZESTĘPSTWA SKIMMINGU

WSTĘP

Rynek obrotu bezgotówkowego to dziś jeden z priorytetów w działalności instytucji finansowych, w tym przede wszystkim banków. Wychodzi bowiem na przeciw ogólnym tendencjom zmieniającego się świata, jak: globalizacja kontaktów międzyludzkich, lawinowy wzrost transakcji handlowych, powszechne zastosowanie Internetu i uznana wartość szybkiego przepływu informacji. Jednym z głównych fundamentów tak pojętego rynku jest karta płatnicza. Chociaż karty takie od początku funkcjonowania narażone były na działania niezgodne z prawem, to dopiero plaga przestępczości skimmingu zmusiła podmioty uczestniczące w obrocie kartowym do radykalnego zwiększenia jego bezpieczeństwa. Głównym problemem stał się pasek magnetyczny, na którym już od pół wieku zapisuje się dane umożliwiające wykonanie transakcji w bankomacie i terminalu POS. Skimming w najprostszym ujęciu polega bowiem na skopiowaniu informacji zapisanej na pasku magnetycznym oryginalnej karty celem wyprodukowania jej

* Paweł Opitek jest doktorantem w Katedrze Kryminalistyki Wydziału Prawa i Administracji Uniwersytetu Śląskiego w Katowicach, a także prokuratorem Prokuratury Rejonowej Kraków – Podgórze w Krakowie.

kopii[1]. W szerszym znaczeniu pod pojęciem tym rozumie się cały proceder przestępczy, który polega ponadto na nielegalnym wykorzystaniu skopiowanych danych, np. poprzez ich sprzedaż w sieci lub bezprawne transakcje w środowisku CNP (z ang. *card not present*, tj. bez fizycznego użycia karty). Okazało się bowiem, że łatwo skopiować informacje umieszczone na pasku magnetycznym i dlatego od kilkunastu lat zachodzą daleko idące zmiany w zakresie funkcjonowania kart płatniczych. W dużej mierze przyczyniło się do tego wdrożenie EMV. Warto więc zadać pytanie, czy implementacja wspomnianego standardu zapewniła bezpieczeństwo transakcjom kartowym, a w szczególności, czy wyeliminowała zagrożenia związane ze skimmingiem?

1. CZYM JEST EMV?

Twórcami EMV były trzy organizacje płatnicze: Europay, MasterCard i Visa, a obecnie program ten zarządzany jest przez spółkę EMVCo, która stanowi współwłasność: American Express, JCB, MasterCard i Visa. Termin „EMV" oznacza globalny standard obsługi płatności przy użyciu kart z mikroprocesorem. Składają się na niego kolejne serie specyfikacji, procesów ich wdrażania i procedur testowych dla mikroprocesorowych kart płatniczych i urządzeń je akceptujących, jak punkty sprzedaży POS i bankomaty. Wspólne założenia techniczne oparte na płatnościach z wykorzystaniem mikroprocesora mają gwarantować kompatybilność kart i przeznaczonych do ich obsługi terminali na całym świecie. Do transakcji dochodzi bowiem w momencie, kiedy mikroprocesor umieszczony w plastikowej karcie lub innym urządzeniu przenośnym (np. telefonie komórkowym) nawiązuje kontakt z terminalem (poprzez fizyczne zetknięcie lub bezstykowo, z wykorzystaniem technologii NFC (z ang. *near field communication*). Chip przechowuje informacje o rachunku bankowym posiadacza karty i za pomocą specjalnej aplikacji wykonuje kryptograficzne przetworzenie danych dla potwierdzenia prawidłowości m.in. numeru karty. W Europie wprowadza się ponadto na klawiaturze terminala kod PIN, który porównywany jest przez system z PIN-em składowanym w procesorze dla zweryfikowania, czy transakcja ma autoryzowany charakter.

Specyfikacje EMV (pierwszą wersję opublikowano w 1994 roku, a najnowsza pochodzi z listopada 2011 roku) opierają się na normie ISO 7816 i określają wzajemne zależności fizyczne, elektryczne i aplikacyjne warunkujące współpracę pomiędzy kartami z chipem a urządzeniami „czytającymi" takie karty w trakcie

[1] W 2012 roku 46% incydentów skimmingu kart płatniczych miało miejsce w bankomatach, a 36% w terminalach POS sprzedaży detalicznej; rok wcześniej 79% wspomnianych incydentów dokonano w terminalach POS; [w:] *Data shows ATM fraud hotspots in US*, Payments cards & mobile 2014/3, s. 14.

realizacji różnego rodzaju transakcji. Chodzi przede wszystkim o proces autoryzowania i uwierzytelnienia płatności z fizycznym użyciem karty (i pominięciem paska magnetycznego) na podstawie danych zawartych w pamięci chipa zatopionego w plastiku[2]. Autoryzacja oznacza w tym przypadku udzielenie zgody na wykonanie transakcji przez płatnika, podczas gdy uwierzytelnienie jest techniczną procedurą weryfikacji realizowaną przez dostawcę usługi. Najogólniej rzecz biorąc, proces uwierzytelnienia następuje poprzez przesłanie z terminala informacji dotyczących karty płatniczej (m.in. jej numeru, daty ważności) do banku oraz wpisanie numeru PIN. Z kolei płatnik (posiadacz karty) dokonuje autoryzacji poprzez wpisanie i potwierdzenie PIN-u. Moment zapłaty kartą za towar/usługę lub jej użycia w bankomacie jest bowiem najbardziej „newralgiczny" pod względem bezpieczeństwa: dochodzi wtedy równocześnie do złożenia zlecenia płatniczego, uwierzytelnienia i autoryzacji. Jeśli przestępcy uda się na tym etapie zrealizować operację, to szanse odzyskania przez bank utraconych środków finansowych maleją niemalże do zera. Dlatego dla ochrony systemu przed transakcjami typu „fraud" niezbędne było ich weryfikowanie w czasie rzeczywistym i obecnie w Europie zdecydowana większość transakcji realizowana jest w trybie online. Obowiązek ich kontroli ciąży przede wszystkim na bankach, centrach rozliczeniowych i podmiotach zarządzających bankomatami, a narzędziem niezmiernie to ułatwiającym jest EMV.

Omawiany standard nie został jednak wprowadzony z dnia na dzień; przeciwnie, proces migracji do EMV ma charakter złożony i dotyczy różnorodnych obszarów na pierwszy rzut oka niewiele mających ze sobą wspólnego. Chociaż niewątpliwie karty są najważniejszym jego elementem, to wprowadzenie EMV wymagało o wiele więcej aniżeli tylko dodania do nich mikroprocesora. Chodziło o unowocześnienie całej infrastruktury związanej z wdrożeniem bezpiecznej technologii i skonfigurowania jej z innymi urządzeniami, jak terminale POS, bankomaty, ale także smartfony, tablety i Internet[3]. Oprócz rozwiązań w zakresie wzrostu bezpieczeństwa, wdrożeniu EMV przyświecają cele czysto komercyjne: nowoczesne karty cechuje duża pojemność zapisu (co umożliwia umieszczenie na nich wielu danych), kompatybilność, a to determinuje wzrost liczby i wartości realizowanych transakcji bezgotówkowych. Z drugiej strony okazało się, że ograniczenia związane z globalną implementacją EMV wynikają m.in. z wysokich kosztów związanych z przebudową infrastruktury technicznej i informatycznej oraz koniecznością wprowadzenia zmian prawnych związanych z funkcjonowaniem kart płatniczych w tym standardzie. Są to procesy czasochłonne, wymagające nakładu ogromnych środków

---

[2] J. Biegański, *Sposoby popełniania przestępstw związanych z elektronicznymi instrumentami płatniczymi po wdrożeniu EMV*, [w:] J. Kosiński (red.), *Przestępczość teleinformatyczna*, Wydawnictwo WSP w Szczytnie, Szczytno 2012, s. 19.

[3] O. Manaham, *EMV: Building the foundation for the future of payments*, Payments Strategy & Systems, 2013/2, s. 183.

finansowych. Nie ułatwia ich brak w skali światowej szczegółowych unormowań dotyczących zasad odpowiedzialności konkretnych podmiotów za niezapewnienie odpowiedniego poziomu ochrony terminalom płatniczym, w tym m.in. obowiązku pokrycia strat powstałych w wyniku oszustwa. Dlatego pierwotny optymizm pokładany w EMV z biegiem czasu przerodził się w żmudny i trwający do dziś proces dostosowania światowej infrastruktury do obsługi kart płatniczych w nowocześniejszym standardzie.

Z perspektywy zwalczania przestępczości kartowej o wiele ważniejszy jest jednak inny skutek wprowadzenia EMV aniżeli względy czysto komercyjne. Ponieważ na pasku magnetycznym znajduje się zakodowana informacja, że na karcie jest chip, to fakt ten utrudnia używanie ich fałszywych klonów. Dzieje się tak, gdyż użycie karty jedynie z paskiem (dane kart podrobionych zapisane są tylko na pasku) w urządzeniu, które potrafi obsłużyć chipa, wiąże się z dużym ryzykiem wykrycia oszustwa przez różnego rodzaju systemy monitorujące (detekcyjne, „antyfraudowe"). Ponadto, nawet bez podejrzenia działania niezgodnego z prawem, wydawca karty może automatycznie odmówić autoryzacji takiej operacji. Okazało się więc, że umieszczenie w budowie karty mikroprocesorowej układu elektronicznego pozwala na zastosowanie nowoczesnych rozwiązań podnoszących poziom bezpieczeństwa transakcji. Jest to jeden z głównych impulsów powszechnego rozwoju technologii EMV.

2. WPŁYW STANDARDU EMV NA PRZESTĘPCZOŚĆ KARTOWĄ

2.1. Ujęcie historyczne

Poczynając od końca lat 90. ubiegłego stulecia kraje Europy Zachodniej zmagały się z plagą przestępczości kartowej, a straty spowodowane oszukańczymi transakcjami bankomatowymi sięgały setek milionów dolarów. Ich lawinowy wzrost nastąpił w latach 2008–2009. Chodziło tu głównie o nielegalne pozyskiwanie w terminalach płatniczych numerów kart i wykorzystywanie ich do oszukańczych transakcji. Krajem najbardziej narażonym na skimming była Wielka Brytania i dlatego tamtejszym instytucjom finansowym szczególnie zależało na wyeliminowaniu niebezpieczeństwa, jakie niósł ze sobą łatwy do skopiowania pasek magnetyczny umieszczony na karcie. W tym celu banki na Wyspach zdecydowały się na wprowadzenia programu o nazwie „Chip and PIN" i jako pierwsze na świecie w pełni implementowały standard EMV. Zakładał on przede wszystkim dodanie mikroprocesora do karty oraz autoryzację numerem PIN każdej operacji w środowisku *card present* (tj. z fizycznym użyciem środka płatniczego). Pierwsze transakcje oparte na nowej technologii przeprowadzono w 2004 roku; w kolejnych latach opisane działania zakończyły się powodzeniem. Począwszy od 2009 r. zdecydowanie zmniejszała się wy-

sokość strat generowanych poprzez bezprawne kopiowanie kart płatniczych: o ile w 2001 roku w Wielkiej Brytanii oszustwa z fizycznym wykorzystaniem fałszywych kart stanowiły 39% ogółu przestępstw kartowych, to w 2011 roku liczba ta wynosiła już „tylko" 11%[4]; z kolei aż o 79% spadła do 2012 roku ogólna liczba incydentów nielegalnego kopiowania pasków magnetycznych i produkcji kart podrobionych[5].

Podobne korzystne pod względem bezpieczeństwa tendencje dało się zaobserwować w skali ogólnoeuropejskiej. Dzięki systematycznej migracji środowiska bankowego do EMV, w Europie Zachodniej począwszy od 2008 roku odnotowano stały spadek liczby transakcji związanych z wypłatą środków pieniężnych z bankomatów przy użyciu „białego plastiku" (tak zwykło się nazywać karty podrobione przez skimmerów). Wynikało to także z zastosowania przez instytucje finansowe coraz bardziej wyrafinowanego oprogramowania i procedur wykrywających oraz przeciwdziałających oszustwom kartowym (m.in. informatycznych systemów detekcji, które w rzeczywistym czasie monitorowały i rozpoznawały podejrzane operacje). Duże znaczenie miało również zacieśnienie współpracy pomiędzy podmiotami uczestniczącymi w rynku kart płatniczych i organami ścigania przestępstw oraz popularyzacja wiedzy wśród klientów detalicznych banków, jak uchronić się przed oszustwami popełnianymi na omawianym polu.

Proces przejścia na nowy standard nie wszędzie jednak przebiegał równomiernie. Przeciwnie, o ile w 2009 roku prawie we wszystkich krajach „starej" Unii bankomaty zostały przystosowane do pracy w EMV, to takie kraje, jak na przykład Polska, były dopiero w połowie drogi wdrażania tego systemu. Co prawda nad Wisłą pierwsza karta z mikroprocesorem została wydana już w latach 90. ubiegłego stulecia, ale nie miała ona nic wspólnego z chipem działającym w EMV. W tej części Europy największa fala migracji dokonała się w latach 2008 i 2009, przy czym jeszcze w 2010 roku duża część ATM-ów (z ang. *automatic teller machine*, tj. bankomat) realizowała wypłaty przy użyciu kart fałszywych. Z informacji opublikowanych przez Związek Banków Polskich wynika, że w Polsce dopiero pod koniec 2011 roku funkcjonowało w EMV 90,43% kart płatniczych, 94% terminali POS i 97% bankomatów[6]. Doszło więc do sytuacji, że przez kilka lat w jednych krajach Europy bankomaty obsługiwały karty płatnicze wyłącznie w standardzie „Chip and PIN", podczas gdy w innych spora część ATM-ów działała cały czas na starych zasadach. Dlatego w latach 2009–2010 nastąpił „pochód" przestępstwa skimmingu w zakresie realizacji nielegalnych wypłat. W Wielkiej Brytanii czy Francji przestępcy nadal zakładali nakładki na bankomaty, kopiowali paski magnetyczne i przechwytywali

---

4 V. Conroy, *Countering the threat of CNP fraud*, Payments Strategy & Systems, 2013/7–8, s. 15.

5 *Fraud. The Facts 2012. The definitive overview of payment industry fraud and measures to prevent it*, The UK Cards Association, London 2012, s. 8.

6 E. Stępnik, *Sprawozdanie z wdrażania SEPA w Polsce w roku 2012*, Związek Banków Polskich, www.sepapolska.pl (dostęp: 17.02.2013).

przypisane im kody PIN (technologia EMV nie chroni użytkownika karty przed takim skopiowaniem), jednak po wypłatę pieniędzy przy użyciu „białego plastiku" przyjeżdżali do krajów Europy Środkowo-Wschodniej. Chodziło głównie o miejsca, w których funkcjonowały jeszcze bankomaty całkowicie poza standardem EMV lub akceptujące tzw. *fallback*. Pojęcie to oznacza systemy honorujące procedurę cofnięcia transakcji bankomatowej do starszej technologii. Może się bowiem zdarzyć, że bankomat przystosowany do EMV zaakceptuje również procedurę *magnetic stripe fallback transactions*, a więc transakcja zostanie dokonana przy użyciu paska magnetycznego w bankomacie zgodnym ze standardem EMV, pomimo że użyto do niej danych z karty, która powinna posiadać mikroprocesor. Ostatecznie to bank decyduje, czy zezwolić na wypłatę gotówki z wykorzystaniem takiej procedury i od sposobu zarządzania ryzykiem operacji elektronicznych w konkretnej instytucji finansowej zależy, czy transakcja poza systemem EMV będzie dopuszczona (z większymi lub mniejszymi ograniczeniami), czy też dojdzie automatycznie do jej odrzucenia.

2.2. Wpływ standardu EMV na przestępczość kartową na świecie

Unowocześnienie działania systemu kart płatniczych w Europie, przy równoczesnej nierównej implementacji EMV na świecie, spowodowało więc, że od kilku lat obserwuje się lawinowy wzrost liczby nielegalnych transakcji dokonywanych poza Unią Europejską z wykorzystaniem danych kart skopiowanych na terenie państw Starego Kontynentu. Fałszywe karty są wykorzystywane w miejscach, gdzie bankomaty dopuszczają transakcje na podstawie paska magnetycznego. W konsekwencji to europejskie banki, których karty są skimmowane, nierzadko odpowiadają finansowo za zaniechania swych zagranicznych odpowiedników i są zobowiązane do pokrycia strat powstałych w wyniku nielegalnych wypłat poza Europą[7]. W przypadku Wielkiej Brytanii straty generowane za granicą z wykorzystaniem kart brytyjskich emitentów wyniosły w 2012 roku 101,3 milionów funtów, chociaż i tak spadły o 56% w porównaniu z ich rekordowym poziomem z roku 2008 (230,1 mln funtów)[8]. Doszło więc do paradoksalnej sytuacji: pomimo ogromnych inwestycji sektora finansowego państw Unii Europejskiej w zmodernizowanie systemu kart płatniczych i wyrugowania z jej terenu nielegalnych wypłat bankomatowych, problem pozostał. Przestępcy mogą nadal realizować oszukańcze transakcje w innych szerokościach geograficznych, a służby policyjne krajów członkowskich UE mają ogromne trudności w skutecznym zwalczaniu tego procederu[9]. Ponadto mieszkańcy Starego Kontynentu są coraz bardziej narażeni na skimming swoich kart płatni-

---

7 *Situation Report. Payment Card Fraud in The European Union. Perspective of Law Enforcement Agencies*, Europol 2012, s. 7–8.

8 *Fraud. The Facts 2013. The definitive overview of payment industry fraud and measures*, The UK Cards Association, London 2013, s. 30.

9 *Situation Report. Payment…*, *op. cit.*, s. 7–8.

czych poza Europą i w tym zakresie stanowią cel dla grup przestępczych. Dotyczy to szczególnie Stanów Zjednoczonych, Ameryki Łacińskiej oraz rejonu Azji i Pacyfiku. Nawet jeśli skopiowana karta jest „odblokowana" do użytku w takim miejscu tylko na czas wakacyjnego wyjazdu czy podróży służbowej, to i tak przestępcy potrafią niezmiernie szybko wyprodukować jej klon i zrealizować wypłatę, zanim prawowity posiadacz środka płatniczego powróci do rodzimego kraju[10].

W konsekwencji skimming kart płatniczych, chociaż zmienił w ostatnich latach swoje oblicze, nadal jest poważnym problemem. Zgodnie z danymi ogłoszonymi przez European ATM Security Team (październik 2013 roku) na podstawie informacji uzyskanych od 19 krajów należących do SEPA[11] i 3 krajów spoza tego obszaru[12], skimming bankomatowy był zgłoszony przez 20 z powyższych państw, przy czym w 8 z nich zanotowano jego wzrost, a w 6 spadek[13]. Tylko 2011 r. łączna suma strat wynikających z nielegalnego wykorzystania kart płatniczych w obrębie SEPA wyniosła 1,16 biliona euro[14]. Odnotowano ponadto dalszy proces migracji skimmingu bankomatowego do obszarów znajdujących się poza *EMV liability shift areas*. Jeśli chodzi o statystykę ogólnoświatową, to od stycznia 2013 roku do września 2013 roku o stratach związanych z omawianym przestępstwem raportowało 38 krajów i terytoriów znajdujących się poza SEPA, łącznie z takimi egzotycznymi miejscami, jak Trinidad i Tobago, Nepal czy Wyspa Świętej Łucji na Morzu Karaibskim[15].

2.3. Wpływ standardu EMV na przestępczość kartową w Polsce

Polska od dawna znajduje się na europejskiej mapie skimmingu, a w latach 2008–2009 odnotowano gwałtowny wzrost incydentów związanych z wypłatą pieniędzy z bankomatów przy wykorzystaniu fałszywych kart płatniczych. Najczęściej wykorzystywano do tego karty emitentów pochodzących z Wielkiej Brytanii, rza-

---

[10] *EAST Publishes European Fraud Update, July 2013*, www.european-atm-security.eu/Press (dostęp: 24.09.2013).

[11] Obszar Jednolitych Płatności w Euro (z ang. *Single Euro Payments Area*) realizowany przez 32 kraje Starego Kontynentu (w tym Polskę) mający za zadanie uprościć i uczynić bardziej efektywnym rynek rozliczeń pieniężnych poprzez stworzenie wspólnych ram organizacyjnych na całym obszarze SEPA.

[12] Chodzi m.in. o następujące kraje: Austrię, Belgię, Kanadę, Danię; Finlandię, Francję, Niemcy, Węgry, Włochy, Polskę, Rumunię, Rosję, Hiszpanię, Szwecję, Szwajcarię, Wielką Brytanię i Ukrainę.

[13] *EAST November 2013 Update*, European ATM Security Team (EAST), www.european-atm-security.eu., data odczytu: 14.03.2014 r. Z krajów obszaru SEPA skimming bankomatowy odnotowano w następujących państwach: Bułgaria, Francja, Włochy, Holandia i Wielka Brytania.

[14] *Second Report on Card Fraud*, European Central Bank, July 2013.

[15] *European Fraud Update 03/2013* prepared by The European ATM Security Team, www.european-atm-security.eu (dostęp: 3.03.2015).

dziej z Norwegii, Finlandii czy Szwecji. Zaledwie kilka procent nielegalnych wypłat dotyczyło kart wydanych przez krajowych emitentów. W tym okresie przestępcy przyjeżdżali do Polski nie tylko wypłacać pieniądze z ATM-ów, ale także skimmować karty na bankomatach zainstalowanych nad Wisłą, a następnie przy użyciu ich kopii dokonywali „fraudowych" transakcji za granicą, najczęściej na terenie Bułgarii i Rumunii. Z czasem polski rynek kart płatniczych stawał się coraz nowocześniejszy, a banki wymieniły karty tylko z paskiem magnetycznym na karty hybrydowe, tj. zaopatrzone zarówno w pasek jak i chipa oraz działające w systemie EMV. Równocześnie do nowego standardu przystosowywano bankomaty, od końca 2012 roku niemal wszystkie funkcjonowały w ulepszonej technologii. Dlatego, o ile do roku 2010 przestępcy przyjeżdżali do Polski przede wszystkim w celu realizacji „fraudowych" wypłat na podstawie sfałszowanych kart pochodzących z innych krajów (najczęściej z Wielkiej Brytanii), o tyle od 2011 roku, z powodu wdrożenia systemu EMV, nad Wisłą „tylko" skimmuje się karty, a wypłaty z wykorzystaniem ich klonów realizowane są poza Europą[16].

Podobne zamiany zachodziły w pozostałych krajach, które podobnie jak Polska z pewnym opóźnieniem modernizowały swoją infrastrukturę do obsługi transakcji kartowych. W konsekwencji podjęte działania bardzo utrudniły dokonywanie oszukańczych wypłat bankomatowych w całej Europie i dały asumpt do kolejnego przetasowania na geograficznej mapie skimmingu, tj. przyczyniły się do dalszej migracji nadużyć kartowych. Kiedy w Unii Europejskiej dostosowano urządzenia do EMV, to przestępcy zaczęli realizować nielegalne wypłaty w tych częściach świata, gdzie bankomaty nadal autoryzowały operacje na podstawie paska magnetycznego: przede wszystkim w Stanach Zjednoczonych Ameryki Północnej, a ponadto w Tajlandii, Kolumbii, Republice Dominikany, Wietnamie, Peru, Brazylii czy Meksyku. Możliwości skutecznego ścigania tego typu przestępstw były bardzo ograniczone: jeśli skimmerzy nie zostanli zatrzymani na gorącym uczynku, to potem bardzo trudno jest kontrolować i przeciwdziałać nielegalnemu wykorzystaniu skradzionych danych kart płatniczych.

3. SZANSE I ZAGROŻENIA ZWIĄZANE Z EMV

Z przeprowadzonej analizy wynika, że na straty spowodowane skimmingiem narażeni są nie tylko obywatele krajów, w których nie implementowano lub implementowano tylko częściowo standard EMV, ale omawiane przestępstwo nadal jest zagrożeniem dla mieszkańców Europy. EMV nie chroni bowiem przed możliwością

[16] Warto zaznaczyć, że chociaż z zapewnień przedstawicieli polskiego sektora bankowego wynika, że krajowe bankomaty realizują wyłącznie transakcje w standardzie EMV, to jednak nie ma 100. procentowej pewności, iż żaden z nich nie dopuszcza procedury *fallbeck*. Wszystko zależy od zarządzania ryzykiem przez konkretną instytucję finansową.

nielegalnego kopiowania pasków magnetycznych, a większość kart funkcjonujących na Starym Kontynencie to karty hybrydowe. Wynika to z ich uniwersalnego charakteru: organizacje płatnicze gwarantują posiadaczom kart możliwość realizacji transakcji w każdym miejscu na świecie, niezależnie od tego, czy np. funkcjonuje tam bankomat w systemie EMV, czy maszyna czyta dane tylko z paska magnetycznego. Co prawda, niektóre banki próbują emitować karty jedynie z mikroprocesorem, ale mają one zawężone pole zastosowania. Stosuje się ponadto inne rozwiązania, jak np. tzw. geobloking, który w najprostszym wydaniu opiera się na oszacowaniu czasu w jakim możliwe jest dokonanie operacji finansowej tą samą kartą pomiędzy dwoma miejscami. Jeżeli pierwszą transakcję wykonano w takiej lokalizacji geograficznej, że niemożliwe byłoby w określonym czasie przemieszczenie się w miejsce drugiej wypłaty, to następuje zablokowanie karty. Rodzaj i forma wprowadzonych zabezpieczeń zależy od wielu czynników, m.in. od tego, czy transakcja dokonywana w EMV jest autoryzowana *online* czy *offline*. W pierwszym przypadku zaszyfrowane dane przesyłane są na bieżąco do emitenta i on w czasie rzeczywistym zezwala na dokonanie operacji kartowej lub ją odrzuca. W transakcji typu *offline* natomiast karta i terminal komunikują się ze sobą („rozmawiają"), następuje weryfikacja karty pod kątem z góry zdefiniowanych przez bank parametrów i od uzyskanych w ten sposób wyników zależy możliwość realizacji zlecenia płatniczego. Autoryzacja *online* jest typowa dla terminali działających w sieci internetowej, na bieżąco łączących się z serwerem banku; rozwiązanie takie daje większe możliwości przeciwdziałania oszustwom, ale także więcej kosztuje (chodzi m.in. o opłaty za transfer informacji). W autoryzacjach *online* stosuje się np. sztuczne sieci neuronowe pozwalające na podstawie analizy i kojarzenia wielu danych segmentować transakcje, grupować je w podobne skupiska i „wyłapywać" na bieżąco transakcje nietypowe, o podwyższonym ryzyku, niepasujące do standardowego zachowania danego konsumenta.

EMV nie chroni natomiast przed innymi nielegalnymi działami wykraczającymi poza moment użycia karty płatniczej w czytniku. Nie niweluje ryzyka przechwycenia danych transmitowanych z wykorzystaniem Internetu pomiędzy terminalem płatniczym a akceptantem (punktem rozliczeniowym). Nie chroni też przed włamaniami do baz emitentów lub innych podmiotów gromadzących informacje o klientach (sprzedawcy przechowują tysiące numerów kart, a wielkie sieci handlowe miliony, np. w celu analizy zachowania konsumentów na rynku). Źródłem wycieku danych o kartach mogą stać się ataki hakerskie i nawet jeśli sprawcy nie przechwycą przypisanych środkom płatniczym PIN-ów, to skradzione informacje i tak nadają się do nielegalnego wykorzystania w środowisku CNP. Dlatego najnowsze tendencje w ochronie omawianych danych (tj. danych o użytkowniku i danych autoryzacyjnych) znacznie wykraczają poza sam moment użycia karty w terminalu, a technologie szyfrowania i tokenizacji neutralizują zagrożenia związane z przechowywaniem i transmisją wrażliwych informacji. Szyfrowanie dokonywane jest

za pomocą specjalnego klucza gruntownie zmieniającego treść przekazu biegnącego z czytnika „plastikowego pieniądza" do terminalu POS lub dalej do głównego serwera emitenta i uniemożliwiającego poprawne (sensowne) odczytanie danych bez zastosowania odpowiedniego algorytmu. Drugi składnik zabezpieczenia, tokenizacja, to proces w trakcie którego numer karty płatniczej zostaje przedstawiony w formie zastępczej (tzw. tokenów) i w ten sposób składowany w bazie danych, prowadzonej w pierwszej kolejności przez merchantów. W ten sposób minimalizuje się ponoszone przez firmę ryzyko naruszenia bezpieczeństwa informacji oraz koszty związane z ich składowaniem.

4. POSTULATY

Rozwiązaniem najkorzystniejszym w zwalczaniu skimmingu byłaby pełna implementacja standardu EMV na całym świecie, a przynajmniej w państwach o zaawansowanych gospodarkach rynkowych. Obecnie, chociaż większość krajów migruje na nowy standard, to jednak procesy z tym związane nie przebiegają równomiernie: niektóre kraje implementowały nowoczesną technologię w całości, inne są w trakcie jej wdrażania, ale są też państwa pozostające całkowicie poza EMV[17]. Dlatego międzynarodowe instytucje finansowe prowadzą nieustanne rozmowy w kierunku ogólnoświatowej implementacji omawianego standardu, ale ich ostateczny rezultat trudno przewidzieć.

EMV zostało niemal całkowicie implementowane w Europie, Kanadzie, Australii oraz w Republice Południowej Afryki. W 2014 roku na podobnym poziomie wdrażania EMV były: Stany Zjednoczone Ameryki Północnej, Chiny i Japonia. Szczególnie newralgicznym obszarem na mapie przestępczości kartowej są Stany Zjednoczone[18]. Niezwykle trudnym zadaniem jest bowiem całkowita implementacja standardu EMV w kraju o rozległym terytorium i olbrzymiej masie terminali POS działających w różnych konfiguracjach, nawet jeśli skimming w USA generuje corocznie ogromne straty finansowe. Na początku 2012 roku została opublikowana „mapa drogowa" migracji USA do nowej technologii zarówno w systemie płatniczym MasterCard jak i Visa. Na jej podstawie już od 12 kwietnia 2013 roku bankomaty i karty debetowe Maestro w bankomatach za oceanem mają obowiązek

[17] W 2014 roku zgodnie z danymi EMVco ponad 41% kart na świecie i ponad 71% terminali rozmieszczonych poza USA działało w standardzie EMV. 62% międzynarodowych transakcji płatniczych było przeprowadzonych kartami z chipem i z użyciem akceptujących ich terminali; [w:] *EMV Background*, www.aurustech.com/emv.html (dostęp: 18.03.2015).

[18] Straty w USA w wyniku przestępczości kartowej wyniosły w 2013 roku 18 bilionów dolarów, z czego szacuje się, że 1/3 tej kwoty była wynikiem użycia kart fałszywych, [w:] R. Sidel, *Why new credit cards may fall short on fraud control*, „The Wall Street Journal", Jan. 4, 2015, www.wsj.com (dostęp: 16.03.2015).

działać w EMV. Oznacza to, że od tej daty podmiot zarządzający amerykańskim bankomatem, który nie obsługuje mikroprocesora, jest odpowiedzialny za potencjalne oszustwo popełnione z wykorzystaniem skopiowanych danych „nieamerykańskiej" karty Maestro zaakceptowanej przez ten ATM. Analogiczne przeniesienie odpowiedzialności agentów rozliczeniowych – posiadaczy terminali POS w sklepach i centrach handlowych – w stosunku do kart Maestro nastąpiło w kwietniu 2015 roku; dla instrumentów MasterCard terminem granicznym jest październik 2015 roku. Tym samym (teoretycznie) od października 2015 roku w Stanach Zjednoczonych po stronie akceptanta powinno zostać powszechnie implementowane EMV. Nie można jednak zapominać, że w państwie tym działa jeszcze kilkadziesiąt tysięcy terminali samoobsługowych usytuowanych m.in. na stacjach benzynowych, parkingach i na poczcie. Urządzenia takie często funkcjonują w trybie *offline*, a więc nie mają technicznych możliwości autoryzacji transakcji w czasie rzeczywistym, i dlatego wydłużono dla nich termin migracji do października 2017 roku.

W Stanach Zjednoczonych dyskusja toczy się ponadto wokół problemu, czy wprowadzić metodę autoryzacji „Chip and PIN" czy „Chip and Signature" (tutaj autoryzacja transakcji następuje na podstawie dokonywanej przez akceptanta weryfikacji podobieństwa podpisu posiadacza umieszczonego na karcie z podpisem nakreślonym na potwierdzeniu transakcji) i na chwilę obecną wydaje się, że większość emitentów wybierze drugą z wymienionych metod. Chociaż autoryzacja „Chip and PIN" uważana jest za nowocześniejszą (została przyjęta m.in. w Europie, Australii i Kanadzie), to powodów wyboru „Chip and Signature" jest kilka. Sądzi się na przykład, że w odróżnieniu od konsumentów w Europie i Australii, duża część posiadaczy kart za oceanem miałaby problem z zapamiętaniem czterocyfrowego kodu, szczególnie, że w ich portfelach znajduje się zazwyczaj kilka kart płatniczych. Kolejną przeszkodę dla weryfikacji transakcji PIN-em stanowiłaby konieczność zainwestowania przez akceptantów znacznych środków w zakup „PIN-padów" (tj. klawiatur do wpisywania kodów autoryzacyjnych).

Pomimo dużych wyzwań związanych z prowadzeniem EMV, Stany Zjednoczone są największym rynkiem, jaki do tej pory emigrował na nowy standard i obecnie trwa tam wymiana kart z paskiem magnetycznym na bardziej bezpieczne karty EMV. Z szacunkowych obliczeń wynika, że na koniec 2015 roku 50% kart (tj. ponad 575 milionów) i połowa terminali płatniczych za oceanem będzie funkcjonowało w ulepszonym systemie. Z drugiej strony już teraz jest niemal pewne, że (w praktyce) migracja USA do EMV w wyznaczonych terminach nie zostanie całkowicie zakończona. Konkluzja taka znajduje szersze rozwinięcie: należy się spodziewać, że pomimo zakrojonych na szeroką skalę działań na rzecz pełnej implementacji EMV na świecie, to nawet za kilka czy kilkanaście lat będzie można wskazać miejsca, w których bankomaty realizują transakcje przy użyciu wyłącznie paska magnetycznego, a więc będą podatne na wypłaty „fraudowe". Chodzić może o lokalizacje, które dziś są nieatrakcyjne dla oszustów i dlatego tamtejsze instytucje finansowe przesu-

nęły zmiany w czasie. Przestępstwo skimmingu ma bowiem tendencje emigrowania do najmniej zabezpieczonego środowiska, szuka luk w systemie obsługi transakcji kartowych, szczególnie tam, gdzie pasek magnetyczny jest akceptowany. Poza tym nie ma na 100% gwarancji, że państwa, które ściśle określiły daty przejścia na EMV, dopełnią w terminie swych zobowiązań w zakresie całej infrastruktury kartowej. Oznacza to, że jeśli bank nie zdąży z migracją, to na niego zostanie przeniesiona odpowiedzialność finansowo-prawna za ewentualne straty wynikające z przestępczego użycia karty. Z drugiej jednak strony ideą funkcjonowania kart płatniczych jest ich uniwersalny charakter, a więc posiadacz karty ma prawo spodziewać się, że przy jej użyciu zrealizuje transakcję w aktualnym miejscu pobytu. Skoro nie sposób przyjąć, że w ciągu kilkunastu najbliższych lat zostanie wprowadzony globalny system EMV, to muszą funkcjonować karty z paskiem magnetycznym i terminale je obsługujące[19]. Opisane tendencje i zjawiska znajdują odzwierciedlenie na polskim rynku kart płatniczych. Nadal opłaca się przestępcom skimmować karty nad Wisłą, aby „skradzione" dane wykorzystać do wypłaty gotówki w innych częściach świata.

PODSUMOWANIE

Rezultaty wdrożenia programu EMV w perspektywie przestępczości kartowej można oceniać w dwojaki sposób: niewątpliwe nowy standard przyczynił się do zwiększenia bezpieczeństwa transakcji dokonywanych z wykorzystaniem kart płatniczych, szczególnie w bankomatach i terminalach POS. Z drugiej jednak strony, pomimo wielu zalet, EMV ma także luki i nie chroni całkowicie przed przestępstwami kartowymi, w tym przed skimmingiem paska magnetycznego oraz przestępstwami dokonywanymi poza tzw. *EMV liability shift region* i stratami z tytułu transakcji typu fallback. Wydaje się, że problem skimmingu rozwiązałaby emisja kart jedynie z chipem (bez paska magnetycznego), lecz wymagałoby to dostosowania infrastruktury kartowej do standardu EMV na całym świecie. W wypowiedziach ekspertów rynków finansowych jako najwcześniejsza data realizacji tego celu pojawia się rok 2018. Jednak i ta data wydaje się z wielu względów iluzoryczna. W tym kontekście znamienna jest wypowiedź Ellen Richey (wysokiego przedstawiciela Visy do spraw bezpieczeństwa): „Byłoby pięknym snem sądzić, że pasek magnetyczny zostanie całkowicie wyeliminowany z karty magnetycznej. W rozsądnej przyszłości może on natomiast stać się elementem pomocniczym (zastępczym) dla funkcjonowania kar-

[19] J. Biegański, *Trendy przestępstw w Europie w kontekście zagrożenia podczas Euro 2012*, [w:] J. Kosiński (red.), *Przestępczość teleinformatyczna*, Wydawnictwo WSP w Szczytnie, Szczytno 2012, s. 102.

ty”[20]. Dlatego problem skimmingu sam nie zniknie i nadal trzeba wypracowywać na wielu płaszczyznach skuteczne metody walki z tym przestępstwem.

Streszczenie

W artykule została omówiona kwestia funkcjonowania kart płatniczych pod kątem bezpieczeństwa transakcji dokonywanych z wykorzystaniem „plastikowego pieniądza”, ze szczególnym uwzględnieniem przestępstwa skimmingu i jego wpływ na zmiany techniczne, organizacyjne i prawne rynku kart płatniczych. Ściśle wiąże się z tym termin EMV, rozumiany jako globalny standard obsługi płatności przy użyciu kart z mikroprocesorem. Przyczynił się on w dużej mierze do zmiany obrazu przestępczości popełnianej na omawianym polu, w tym przede wszystkim migracji oszustw kartowych z jednych obszarów geograficznych do innych.

Słowa kluczowe: karta płatnicza, skimming, przestępstwo, EMV, pasek magnetyczny, mikroprocesor, „Chip and PIN”, bank, ATM, transakcja płatnicza, bezpieczeństwo, oszustwo

Abstract

The present article discusses the issue of credit card operation on the market, taking into account transactions performed with the usage of “plastic money”. The crucial aspect here is the crime of “skimming” and its influence on the technical, organisational and legal changes made in the institution of the credit card. The term EMV is strictly connected with this issue as a global standard of payment service with the use of microprocessor cards. It significantly contributed to the changes in the crime map in the field discussed, in particular, to the migration of card frauds from one geographical area to another.

Key words: credit card, skimming, fraud, EMV, magnetic strip, microprocessor, PIN, bank, ATM, payment transaction, safety, fraud

[20] *Card crime fighter: Visa's Ellen Richey by Nadii Oehlsen*, Cards & Payments, June/July 2009, Vol. 22, No. 6.

Bibliografia

Biegański J., *Trendy przestępstw w Europie w kontekście zagrożenia podczas Euro 2012*, [w:] J. Kosiński (red.), *Przestępczość teleinformatyczna*, Wydawnictwo WSP w Szczytnie, Szczytno 2012.

Biegański J., *Sposoby popełniania przestępstw związanych z elektronicznymi instrumentami płatniczymi po wdrożeniu EMV*, [w:] J. Kosiński (red.), *Przestępczość teleinformatyczna*, Wydawnictwo WSP w Szczytnie, Szczytno 2012.

Card crime fighter: Visa's Ellen Richey by Nadii Oehlsen, „Cards & Payments", June/July 2009, Vol. 22, No. 6.

Conroy V., *Countering the threat of CNP fraud*, Payments Strategy & Systems, 2013/7–8.

Data shows ATM fraud hotspots in US, Payments cards & mobile 2014/3.

EAST Publishes European Fraud Update, July 2013, www.european-atm-security.eu/Press (dostęp: 24.09.2013).

EAST November 2013 Update, European ATM Security Team (EAST), www.european-atm-security.eu (dostęp: 14.03.2014).

EMV Background, www.aurustech.com/emv.html (dostęp: 18.03.2015).

European Fraud Update 03/2013 prepared by The European ATM Security Team, www.european-atm-security.eu (dostęp: 3.03.2015).

Fraud. The Facts 2012. The definitive overview of payment industry fraud and measures to prevent it, The UK Cards Association, London 2012.

Fraud. The Facts 2013. The definitive overview of payment industry fraud and measures, The UK Cards Association, London 2013.

Manaham O., *EMV: Building the foundation for the future of payments*, Payments Strategy & Systems, 2013/2.

Second Report on Card Fraud, European Central Bank, July 2013.

Sidel R., *Why new credit cards may fall short on fraud control*, „The Wall Street Journal", Jan. 4, 2015, www.wsj.com (dostęp: 16.03.2015).

Situation Report. Payment Card Fraud in The European Union. Perspective of Law Enforcement Agencies, Europol 2012.

Stępnik E., *Sprawozdanie z wdrażania SEPA w Polsce w roku 2012*, Związek Banków Polskich, www.sepapolska.pl (dostęp: 17.02.2013).