Krzysztof Mikołajczyk

Przestępstwa związane z wykorzystaniem bankowości elektronicznej – skimming

Definicja

Przestępstwa popełniane z wykorzystaniem kart płatniczych stały się w ostatnich latach poważnym zagrożeniem zarówno dla posiadaczy kart, jak i dla bezpieczeństwa całego systemu bankowego. Prężny rozwój elektronicznych produktów bankowych, a zwłaszcza kart płatniczych, mimo że niesie wiele niezaprzeczalnych korzyści, to przyczynia się również do zwiększenia zjawisk przestępczych w tej dziedzinie. Masowość i powszechność stosowania kart płatniczych sprzyja wzrostowi przestępstw z ich użyciem. Najbardziej rozpowszechnionym, a zarazem najniebezpieczniejszym typem przestępstw dokonywanych z wykorzystaniem kart płatniczych, jest tzw. skimming. Należy zaznaczyć, że nie istnieje definicja legalna tego terminu. Etymologia pojęcia s k i m m i n g wywodzi się z angielskiego czasownika *skim*, oznaczającego „zbierać", „pobieżnie przeglądać"[1]. W literaturze przedmiotu występuje wiele definicji niniejszego zjawiska. Najbardziej trafnym opisem będzie określenie s k i m m i n g u jako bezprawnego skopiowania informacji zapisanych na pasku magnetycznym umieszczonym na karcie płatniczej oraz przechwycenie zabezpieczającego kodu PIN, bez wiedzy i woli jej posiadacza lub użytkownika, w celu wykonania duplikatu karty służącego do obciążenia rachunku bankowego posiadacza. Informacje uzyskane przez zeskanowanie ich z paska magnetycznego karty płatniczej posiadacza są umieszczane na sztucznej karcie, tzw. białej karcie (*white plastic*), lub na oryginalnej karcie płatniczej uzyskanej najczęściej w wyniku przestępstwa. Jak już wspomniano na wstępie zjawisko skimmingu wywiera niekorzystny wpływ na cały rynek kart płatniczych, uderzając w wiele podmiotów: posiadaczy kart płatniczych, akceptantów, wydawców i agentów rozliczeniowych. W przypadku gdy występowanie tego przestępstwa się nasila, może ono doprowadzić do spadku zaufania użytkowników systemów kart płatniczych do bezpieczeństwa i prawidłowego funkcjonowania tegoż systemu. Ponadto z punktu widzenia indywidualnego posiadacza karty najdotkliwszym skutkiem skimmingu jest utrata środków finansowych. Z kolei z punktu widzenia wydawców kart szkody związane z tym przestępstwem skutkują obowiązkiem zwrotu posiadaczowi karty równowartości kwoty nieautoryzowanych transakcji oraz, w szerszym ujęciu, powodują spadek zysku z uwagi na zmniejszoną podaż kart.

Pojęcie karty płatniczej

Na przestrzeni ostatnich lat pojęcie karty płatniczej ulegało zmianom, przy czym jego aktualna definicja znajduje się w *Ustawie z dnia 19 sierpnia 2011 r. o usługach płatniczych* (Dz.U. z 2011 r. Nr 199, poz. 1175). Zgodnie z brzmieniem art. 2 pkt 15a tej ustawy *karta płatnicza 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*[2].

[1] Zob. J. Fisiak i in., *Słownik współczesny angielsko-polski, polsko-angielski*, Warszawa 2006, Longman–Pearson, s. 403.

[2] Przytoczona definicja karty płatniczej zastąpiła definicję uprzednio obowiązującą na gruncie *Ustawy z*

Rodzaje kart płatniczych

W literaturze przedmiotu można spotkać wiele sposobów klasyfikowania kart płatniczych, co jest połączone z mnogością rodzajów kart funkcjonujących w obrocie. I tak, zdaniem P. Podsiedlika i T. Czyloka rozróżniamy podział kart z uwagi na funkcjonalność, sposób rozliczania transakcji i ze względu na technologię ich wykonania[3]. Z kolei M. Zajda klasyfikuje karty płatnicze z uwagi na: emitenta, osobę posiadacza, funkcje tych kart, ich cechy techniczne, charakter umowy pomiędzy posiadaczem a emitentem oraz według segmentacji klientów[4]. Jeszcze inny podział proponują R. Kaszubski i Ł. Obzejta, którzy wyodrębniają rodzaje kart płatniczych ze względu na: wydawcę, liczbę podmiotów zaangażowanych w system kart płatniczych, sposób dokonywania płatności, zakres terytorialny użycia karty, termin płatności, technologię zapisu danych na karcie oraz posiadacza[5]. W polskich przepisach prawnych legislator nie dokonał klasyfikacji kart płatniczych, chociaż z definicji legalnych obowiązujących w kolejnych aktach prawnych rangi ustawowej, w tym: w *Ustawie z dnia 29 sierpnia 1997 r. – Prawo bankowe* (Dz.U. z 1997 r. Nr 140, poz. 939), *Ustawie z dnia 19 sierpnia 2011 r. o usługach płatniczych* (Dz.U. z 2011 r. Nr 199, poz. 1175) i *Ustawie z dnia 12 września 2002 r. o elektronicznych instrumentach płatniczych* (Dz.U. z 2002 r. Nr 169, poz. 1385), można by było pokusić się o próbę doktrynalnego podziału na karty płatnicze sensu stricto, karty bankomatowe i karty kredytowe[6]. Rezygnacja ustawodawcy z wyszczególnienia rodzajów kart płatniczych w aktach prawnych była zapewne podyktowana potrzebą stabilizacji przepisów prawa, zważywszy na szybki postęp technologiczny, szczególnie wyrazisty w sektorze bankowości elektronicznej.

Z punktu widzenia poruszanej tematyki klasyfikacja zaproponowana przez R. Kaszubskiego i Ł. Obzejtę jest najbardziej interesująca. Warto zwłaszcza przyjrzeć się podziałowi kart płatniczych z uwagi na sposób dokonywania płatności. Do tej kategorii kart płatniczych zaliczamy:

- **kartę debetową** – jest ona powiązana z rachunkiem płatniczym posiadacza karty i służy do wykonywania transakcji płatniczych. Można się nią posługiwać do wysokości salda dostępnych środków pieniężnych powiększonego o dopuszczalny, dostępny limit zadłużenia (debet). Umożliwia ona również wypłatę gotówki z bankomatu,
- **kartę kredytową** – jest to karta, której uzyskanie nie wiąże się z koniecznością otwierania rachunku oszczędnościowo-rozliczeniowego w banku. Posiadacz karty może wykonywać transakcje do wysokości limitu rachunku kredytowego,
- **kartę obciążeniową** – jest to zmodyfikowany rodzaj karty kredytowej, z odroczonym terminem płatności. Warunkiem jej wydania jest posiadanie rachunku w danym banku przez określony czas. Na podstawie miesięcznych wpływów na

dnia 12 września 2002 r. o elektronicznych instrumentach płatniczych (Dz.U. Nr 169, poz. 1385), zamieszczoną w art. 2 pkt 7. Ustawa ta definiuje kartę płatniczą jako kartę identyfikującą wydawcę i upoważnionego posiadacza, uprawniającą 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.

[3] P. Podsiedlik, T. Czylok, *Przestępczość w bankowości elektronicznej*, Katowice 2010, WSP w Katowicach, s. 10 i nast.

[4] M. Zajda, *Prawno-kryminalistyczne aspekty przestępczości z użyciem elektronicznych instrumentów płatniczych,* Słupsk 2003, Szkoła Policji w Słupsku, s. 12 i nast.

[5] R. Kaszubski, Ł. Obzejta, *Karty płatnicze w Polsce,* Warszawa 2012, Wolters Kluwer, s. 60 i nast.

[6] J. Błachut, *Dokument jako przedmiot ochrony prawnokarnej*, Warszawa 2011, Wolters Kluwer, s. 179.

rachunek osobisty bank określa limit środków, które może udostępnić posiadaczowi karty. Występuje tu konieczność spłacania kredytu przez płatności kartą w krótkich odstępach czasu (najczęściej raz w miesiącu),

- **kartę bankomatową** – jest to karta płatnicza służąca wyłącznie do dokonywania wypłat gotówki z bankomatu lub innego urządzenia z funkcją wypłaty gotówki i dokonywania innych operacji bankowych. Z uwagi na niską funkcjonalność tego rodzaju kart (brak możliwości dokonywania płatności bezgotówkowych), w obrocie praktycznie już się ich nie spotyka,
- **kartę przedpłaconą** – tzw. elektroniczną portmonetkę. Cechą tej karty jest to, że środki pieniężne są zakodowane wewnątrz karty w postaci odpowiednich jednostek (impulsów), a nie ulokowane na rachunku bankowym,
- **kartę wirtualną** – jest ona przeznaczona do użytku wyłącznie w Internecie (bez fizycznego użycia karty, nie musi występować w postaci materialnego nośnika). Karta taka istnieje wyłącznie jako numer rachunku bankowego, który jest wykorzystywany do płatności dokonywanych za pośrednictwem Internetu.

W odniesieniu do skimmingu warto zwrócić uwagę na podział kart płatniczych z uwagi na technologię zapisu danych na karcie. Wyróżniamy zatem:

- **kartę tłoczoną** – jest to karta o najstarszym rodowodzie; wszystkie dane posiadacza są na nią naniesione poprzez wytłoczenie lub wykonanie termodruku. W praktyce karta ta wychodzi z użycia,
- **kartę magnetyczną** – w przypadku tej karty informacje o niej i jej posiadaczu także są zapisywane na pasku magnetycznym. Karty tego typu są coraz częściej zastępowane przez karty mikroprocesorowe, ponieważ technologia zastosowana w przypadku kart magnetycznych jest przestarzała i nie zapewnia dostatecznego poziomu bezpieczeństwa, co wiąże się z łatwością kopiowania paska magnetycznego,
- **kartę mikroprocesorową** (mikrochipową) – w tym przypadku informacje o posiadaczu karty i o niej samej są zawarte w mikroprocesorze wbudowanym w kartę. Dzięki szyfrowaniu danych za pomocą szeregu algorytmów technologia ta jest bezpieczniejsza od rozwiązań zastosowanych w kartach magnetycznych, co więcej, oferuje ona zwiększoną pojemność i funkcjonalność,
- **kartę hybrydową** – stanowi ona etap przejściowy pomiędzy kartami magnetycznymi a kartami mikroprocesorowymi. Wszelkie dane o posiadaczu karty, jak i o niej samej, są zapisywane równolegle w mikroprocesorze i na pasku magnetycznym. Z jednej strony tego typu karta jest odpowiedzią na konieczność dostosowania polskiego rynku kart płatniczych do wymogów SEPA[7], a z drugiej – do niewystarczającej liczby terminali płatniczych obsługujących karty w technologii mikroprocesorowej. Dodatkowym argumentem uzasadniającym funkcjonowanie kart hybrydowych jest możliwość realizowania płatności w krajach trzecich, gdzie dominuje technologia kart magnetycznych.

[7] Jednolity Obszar Płatniczy w Euro (SEPA) – wizja stworzenia obszaru, w którego ramach obywatele, przedsiębiorcy i inne podmioty mogą dokonywać bezgotówkowych rozliczeń w walucie euro na obszarze Europy transgranicznie i w granicach państw członkowskich, według takich samych zasad, regulacji prawnych i zobowiązań.

Rodzaje przestępstw dokonywanych za pomocą kart płatniczych

Zgodnie z poglądem R. Kaszubskiego i Ł. Obzejty przestępczość z wykorzystaniem kart płatniczych nie jest ustawowo zdefiniowana, co więcej, przestępstwa dokonywane przy pomocy tego typu kart są kwalifikowane na podstawie różnych przepisów prawa karnego. Według autorów *przestępczość na kartach płatniczych to wszelka działalność podejmowana przez osoby nieuprawnione lub uprawnione do używania karty płatniczej, mająca na celu uzyskanie dostępu do środków finansowych, w oparciu o które funkcjonuje karta, przez osobę nieuprawnioną lub niezgodne z prawem dokonanie transakcji z wykorzystaniem tych środków*[8]. Zbiór czynności składających się na przestępstwo, o którym mowa, nie został zamknięty ze względu na mnogość form tego typu przestępstw. W doktrynie występuje wiele podziałów i klasyfikacji przestępstw związanych z kartami płatniczymi. Do tego rodzaju przestępstw zaliczamy m.in.:

- **kradzież karty oraz wykorzystanie karty zgubionej** – wejście w posiadanie takiej karty następuje między innymi w wyniku kradzieży, przywłaszczenia, kradzieży z włamaniem czy też sporadycznie – rozboju. Cechą wspólną w przypadku tej kategorii przestępstw jest to, że sprawca po wejściu w posiadanie karty podszywa się pod jej autentycznego posiadacza bez konieczności zmiany danych zamieszczonych na karcie,
- **posługiwanie się kartami doręczonymi** – jest to rodzaj przestępstwa polegającego na przejęciu przez osobę nieuprawnioną karty wysłanej pocztą przez bank do jej użytkownika. W praktyce zdarza się, że pracownicy sektora bankowego, z pominięciem procedur bankowych, wysyłają kody zabezpieczające do karty wraz z samą kartą. Bolączką tego typu przestępstwa jest to, że ujawnienie nieuprawnionych transakcji dokonywanych przy wykorzystaniu przechwyconej karty następuje zazwyczaj po dłuższym czasie,
- **wyłudzenie karty na podstawie wniosku zawierającego fałszywe dane bądź wystawionego na podstawioną osobę** – jest to przestępstwo polegające na złożeniu do banku dokumentów zawierających fałszywe dane, w celu otrzymania oryginalnej karty. Następnie przestępcy posługują się wyłudzoną kartą, dokonując początkowo transakcji na duże kwoty, a następnie poniżej limitów autoryzacyjnych bądź dokonują sfałszowania karty,
- **nielegalne wykorzystanie numeru karty (*carding*)** – polega na posługiwaniu się umieszczonymi na karcie danymi bez zgody jej posiadacza przy dokonywaniu zamówień pocztowych, telefonicznych czy internetowych, niewymagających fizycznej obecności właściciela karty. Warto przy tym zauważyć, że spisanie numerów kart nie jest przestępstwem; dopiero nielegalne wykorzystanie tych numerów rodzi skutki prawne. Sprawcy tego przestępstwa zdobywają dane z karty najczęściej albo przez fizyczny z nią kontakt, albo za pośrednictwem Internetu (np. za pomocą tzw. *hackingu* – kradzieży numeru karty z komputera posiadacza lub z ogólnej bazy danych. Dane z karty można zdobyć również ze stron internetowych, na których przestępcy umieszczają prawdziwe numery kart płatniczych, bądź za pomocą programów komputerowych do generowania numerów kart na podstawie różnego rodzaju algorytmów),

[8] R. Kaszubski, Ł. Obzejta, *Karty płatnicze...*, s. 378.

- **wyłudzenie towarów i usług przez legalnego posiadacza karty** – posiadacz karty kupuje towar lub usługę, wyegzekwowanie od niego zapłaty nie jest jednak możliwe, ponieważ celowo zmienia on miejsce pobytu, nie informując o tym wydawcy karty i nie zwracając tejże karty do wydawcy,
- ***phishing*** – jest formą oszustwa mającego na celu kradzież tożsamości. Polega na podszywaniu się pod znane adresatowi osoby lub firmy w celu nakłonienia go do ujawnienia poufnych danych, takich jak numery kart kredytowych i debetowych lub haseł do konta. Najczęściej tego typu oszustwo jest oparte na wysyłaniu fałszywej wiadomości e-mail, która rzekomo została przekazana przez znaną firmę. Tego typu operacje mogą być również przeprowadzane osobiście, telefonicznie, za pomocą wyskakujących okienek oraz witryn internetowych,
- **fałszowanie kart płatniczych** – grupa działań przestępczych obejmujących podrabianie kart, ich przerabianie, stosowanie tzw. białego plastiku (*white plastic*) oraz dokonywanie fałszerstw elektronicznych, w tym głównie skimming. Podrabianie kart płatniczych polega na wykonaniu duplikatu na podstawie oryginalnej karty (jest jednoznaczne z produkcją zupełnie nowej karty), przerobienie zaś polega na dokonaniu zmian danych na oryginalnych kartach, szczególnie na zmianie tłoczenia numerów, zmianie daty ważności karty, zaprasowaniu starego numeru i wybiciu nowego, wycięciu i doklejeniu odpowiednich elementów karty, dokonaniu zmiany na pasku przeznaczonym na podpis właściciela polegającej na zerwaniu, wytrawieniu bądź zaklejeniu nowymi paskami.

Rodzaje skimmingu

Skimming bankomatowy

Skimming bankomatowy jest przestępstwem polegającym na nielegalnej modyfikacji budowy bankomatu w celu przechwycenia kodu PIN oraz danych z paska magnetycznego karty płatniczej, aby wykonać jej duplikat, który będzie służyć do wypłaty środków pieniężnych z rachunku bankowego, do którego przypisana jest dana karta. Modyfikacji bankomatu dokonuje się głównie przez umieszczenie urządzenia skanującego kartę, tzw. skimmera, na otworze, do którego wsuwa się karty. Profesjonalne nakładki to miniaturowe urządzenia mogące zarówno przesyłać dane drogą radiową, jak i zapamiętywać dane na wbudowanej karcie pamięci.

Zdjęcie 1. Przykład modyfikacji bankomatu umożliwiający skimming.

Źródło: https://www.google.pl/ [dostęp: 15 XI 2012].

Najistotniejsze z punktu widzenia osoby dopuszczającej się skimmingu jest zeskanowanie informacji zawartych na drugiej ścieżce paska magnetycznego, która umożliwia realizację transakcji w terminalach sklepowych POS i wypłatę środków pieniężnych z bankomatu. *Pasek magnetyczny oryginalnej karty płatniczej zawiera 3 ścieżki: na pierwszej zapisane w formie jawnej jest imię i nazwisko posiadacza karty, suma kontrolna, dane kraju i banku wydającego kartę; na drugiej znajduje się numer karty, data ważności i kod serwisowy do prawidłowego odczytu; trzecia*

ścieżka pozostaje praktycznie niewykorzystana[9]. Dane pochodzące z zeskanowanego paska magnetycznego karty są nagrywane na chip znajdujący się w skimmerze lub automatycznie przesyłane przez to urządzenie do komputera przenośnego obsługiwanego przez przestępcę w pobliżu bankomatu.

Kolejnym niezbędnym elementem modyfikacji bankomatu jest zainstalowanie kamery o niewielkich rozmiarach lub specjalnej nakładki na klawiaturę bankomatu. Oba te urządzenia służą jednemu celowi, mianowicie uzyskaniu numeru kodu zabezpieczającego PIN. Wspomniane nakładki na klawiaturę bankomatu mają wbudowany mechanizm informatyczny, który przesyła dane w postaci dźwięków właściwych dla poszczególnych cyfr do umieszczonego w niewielkiej odległości czytnika, który je zapisuje w odpowiedniej kolejności. Informacje z zeskanowanych kart są bezpośrednio nagrywane na tzw. białe karty lub oryginalne karty płatnicze, bądź na karty, które swoim klientom oferują m.in. stacje paliw, pralnie czy hipermarkety. Przestępcy mogą nagrać pozyskane nielegalnie informacje na kartę chociażby przy użyciu ogólnodostępnych urządzeń, np. kodera kart magnetycznych, który jest dostępny w legalnym obrocie. Jego całkowity koszt wynosi około 2000 zł. Następnie, w sprzyjających dla siebie warunkach, sprawcy demontują skimmer oraz kamerę bądź nakładkę na klawiaturę. Szczególną formą tego typu przestępstwa jest podrabianie kart za pomocą skopiowania zapisu ścieżki magnetycznej karty na tzw. białą kartę (*white plastic*). Jest to kawałek białego plastiku wielkości karty płatniczej, na który nanoszone są wytłoczenia z właściwymi danymi. W przypadku umieszczenia na pasku magnetycznym dodatkowych danych uzyskanych w sposób nielegalny występuje tzw. fałszerstwo całkowite metodą białego plastiku. Należy zaznaczyć, że karty tego typu są ogólnodostępne w obrocie handlowym.

Zdjęcie 2. Biała karta (*white plastic*).
Źródło: https://www.google.pl/ [dostęp: 15 XI 2012].

W momencie uzyskania kompletu umożliwiającego przestępcom nieuprawnione obciążenie rachunku posiadacza karty w postaci „sklonowanej" karty wraz z kodem

[9] *Wyrok SA we Wrocławiu z dnia 11 lipca 2008 r.*, II AKa 143/08, „Biuletyn Sądu Apelacyjnego we Wrocławiu" 2009, nr 3 (11), s. 16.

PIN, najczęściej dokonują oni wypłat gotówki z bankomatów lub posługują się tą kartą w punktach usługowo-handlowych, albo też dokonują ich sprzedaży innym przestępcom, najczęściej za pośrednictwem nielegalnych stron internetowych.

Z modyfikacją bankomatu są również związane inne typy przestępstw niemieszczące się w zakresie typowego skimmingu. Do ciekawszych przykładów modyfikacji bankomatu należy między innymi tzw. pętla libańska lub tzw. libijskie oczko, polegające na zablokowaniu otworu bankomatu za pomocą plastikowej folii, co skutkuje zablokowaniem karty osoby próbującej dokonać operacji bankomatowej. W momencie pojawienia się problemów ze zwrotem karty przestępca podchodzi do ofiary, oferując pomoc w odzyskaniu karty. Pokrzywdzony najczęściej podaje przestępcy numer PIN. Po pozorowanej, nieudanej próbie pomocy w wydobyciu karty pokrzywdzony odchodzi od bankomatu, umożliwiając tym samym wydobycie karty przez sprawcę, a następnie jej użycie.

Nielegalna modyfikacja bankomatu może polegać również na zablokowaniu wylotu na banknoty, co powoduje, że posiadacz karty dokonuje prawidłowej z punktu widzenia systemu bankowego operacji finansowej, ale nie otrzymuje zadeklarowanej gotówki, którą po usunięciu blokady pobiera przestępca. Praktyka zna również przypadki podstawiania skonstruowanych przez przestępców fałszywych bankomatów imitujących prawdziwe bankomaty.

Skimming w punktach usługowo-handlowych

Istotą skimmingu w punktach usługowo-handlowych jest zeskanowanie informacji zapisanych na pasku magnetycznym karty płatniczej w momencie dokonywania transakcji tą kartą przez jej posiadacza. Szczególnie często dochodzi do skimmingu w barach, restauracjach i na stacjach benzynowych, a także w innych miejscach, w których karta znika choćby na chwilę z pola widzenia jej właściciela, przykładowo pod pozorem dokonania autoryzacji transakcji lub weryfikacji zgodności danych. Karta jest kopiowana przez sprzedawcę, który współpracuje z przestępcami lub sam jest przestępcą. Przestępcy zdobywają kod PIN, podglądając wpisywany przez posiadacza karty numer na klawiaturze *PIN pad*. Może tego dokonać przykładowo osoba trzecia zaangażowana w proceder bądź osoba obsługująca terminal w punkcie usługowo-handlowym. Warto zauważyć, że obecnie zeskanowanie paska magnetycznego nie nastręcza większych trudności – wystarczy przesunąć kartę płatniczą po powierzchni urządzenia skanującego, którego rozmiary są tak niewielkie, że można je umieścić chociażby w kieszeni spodni. W tym wypadku skanowanie będzie skuteczne poprzez samo zbliżenie karty płatniczej do kieszeni spodni. Końcowy etap tego typu skimmingu jest analogiczny do skimmingu bankomatowego: zeskanowany pasek magnetyczny jest nagrywany na białą czystą kartę magnetyczną lub na oryginalną kartę płatniczą, pochodzącą przykładowo z kradzieży, czy też na jedną z kart, które oferują swoim klientom m.in. stacje paliw, pralnie czy hipermarkety. Użycie karty typu *white plastic* wymaga współpracy przestępcy z akceptantem obsługującym terminal płatniczy POS. Przy braku takiej współpracy sprawca jest zmuszony wgrać dane zeskanowanego paska na oryginalną kartę płatniczą, co utrudnia wykrycie przestępstwa przez akceptanta, chociaż ma on możliwość wykrycia tego procederu, porównując dane wytłoczone na karcie z danymi z paska magnetycznego, wyświetlonymi na monitorze komputera bądź widniejącymi na wydruku transakcji z terminala POS w punkcie handlowo-usługowym, co będzie wskazywało na ich niezgodność.

Zwalczanie skimmingu

Z uwagi na powszechność skimmingu, jego znaczny ciężar gatunkowy oraz dużą liczbę potencjalnych pokrzywdzonych proceder ten jest zwalczany na wielu płaszczyznach, przy zaangażowaniu licznych podmiotów i instytucji. Uwzględniając powyższe, można wyróżnić trzy zasadnicze metody zwalczania skimmingu.

1. Zwiększanie poziomu technologicznego zaawansowania zabezpieczeń kart płatniczych oraz urządzeń służących do ich obsługi, w tym między innymi bankomatów i terminali płatniczych. Proces ten jest długotrwały i stopniowy z uwagi na jego kosztowność i międzynarodowy zasięg, łączy się bowiem z koniecznością wymiany lub udoskonalenia całej infrastruktury obsługującej karty płatnicze. Skimming kart płatniczych jest przede wszystkim wynikiem stosowania na nich przestarzałej technologii paska magnetycznego. Całkowite wyeliminowanie tego zjawiska nastąpi dopiero wtedy, gdy z kart całkowicie znikną paski, które zastąpi technologia mikroprocesorowa. W tym miejscu warto podkreślić, że występujące obecnie, również w Polsce, karty hybrydowe, nie eliminują zagrożenia skimmingiem, a jedynie go minimalizują. Z jednej strony karty te są bezpieczniejsze i bardziej zaawansowane technologicznie niż karty z paskiem magnetycznym, ale z drugiej strony charakteryzują się niższym stopniem zabezpieczenia niż karty z mikroprocesorem. Konieczność używania kart hybrydowych determinuje przestarzała infrastruktura przeznaczona do obsługi kart płatniczych, m.in. terminale i bankomaty. Pierwszym krokiem, który należy zrobić w walce z plagą skimmingu, będzie unowocześnienie tejże infrastruktury. Dopiero później będzie możliwe wprowadzenie kart wyłącznie mikroprocesorowych. Trzeba mieć przy tym świadomość tego, że nie ma systemów całkowicie odpornych na zachowania wypełniające znamiona przestępstw. Obecnie pojawiają się w mediach pierwsze sygnały o nowatorskich sposobach obejścia zabezpieczeń kart mikroprocesorowych, co nie powinno dziwić, biorąc pod uwagę to, że jest to wynik nieustannego „technologicznego wyścigu" świata przestępczego z rozwiązaniami technologicznymi ogólnie pojętego sektora bankowego.

2. Równie ważnym aspektem zwalczania skimmingu jest edukacja uczestników obrotu kartami, głównie posiadaczy kart płatniczych i akceptantów. Z punktu widzenia skuteczności zwalczania skimmingu korzystniejsze wydaje się zapobieganie temu zjawisku, czyli polityka prewencyjna, niż zwalczanie jej skutków. Stąd też warto pokusić się o sformułowanie katalogu zachowań służących zapobieganiu skimmingowi.

Zasady bezpieczeństwa dla akceptanta:

- konieczność zweryfikowania wyglądu karty w celu ujawnienia śladów mogących świadczyć o jej przerobieniu lub podrobieniu,
- weryfikacja danych umieszczonych na karcie płatniczej polegająca na porównaniu danych wytłoczonych na karcie z danymi z paska magnetycznego, wyświetlonymi na monitorze komputera bądź widniejącymi na wydruku transakcji z terminala POS,
- w przypadku zamieszczenia wizerunku posiadacza na karcie płatniczej – porównanie wizerunku z wyglądem osoby dysponującej kartą,
- w razie pojawienia się jakichkolwiek wątpliwości należy zażądać okazania dokumentu potwierdzającego tożsamość.

W przypadku wykrycia jakichkolwiek niezgodności akceptant powinien zatrzymać kartę i poinformować o zaistniałej sytuacji wydawcę karty lub agenta rozliczeniowego.

Zasady bezpieczeństwa dla posiadacza karty:

- przed dokonaniem transakcji w bankomacie posiadacz karty powinien sprawdzić, czy czytnik kart nie wygląda podejrzanie (najczęściej wlot na karty płatnicze w oryginalnych bankomatach jest wklęsły), czy klawiatura bankomatu jest równa lub lekko obniżona w stosunku do poziomu obudowy oraz czy do bankomatu nie są przyklejone podejrzane urządzenia, np. odstające elementy,
- posiadacz karty, wprowadzając kod PIN, powinien zawsze zasłaniać klawiaturę ręką, i to w taki sposób, by nie można go było podejrzeć z żadnej strony,
- w miarę możliwości posiadacz powinien korzystać z bankomatów zlokalizowanych wewnątrz obiektów usługowo-handlowych, które co do zasady są obarczone mniejszym ryzykiem modyfikacji do celów przestępczych (system monitoringu wizyjnego, obecność pracowników agencji ochrony, ograniczony czasowo dostęp z zewnątrz, duże natężenie ruchu osób postronnych),
- systematyczne i częste kontrolowanie stanu salda rachunku bankowego oraz śledzenie historii transakcji,
- ograniczenie ilości wypłat dokonywanych w nocy i po zapadnięciu zmroku,
- w przypadku dokonywania płatności kartą płatniczą należy zwrócić uwagę na podejrzane zachowanie się akceptanta, ewentualnie innych osób z jego otoczenia, które może polegać przykładowo na umieszczaniu karty w innych urządzeniach niż terminal POS czy wychodzeniu akceptanta z kartą do miejsc znajdujących się poza zasięgiem wzroku posiadacza karty.

3. Kolejną metodą zwalczania skimmingu są działania instytucji szczególnie zainteresowanych zwalczaniem tego procederu, takich jak przedstawiciele organów ścigania i banki. Na skuteczność zwalczania tego zjawiska niebagatelny wpływ ma współpraca tych podmiotów zarówno w zakresie edukacyjnym, jak i wymiany informacji. Jako przykład takiej współpracy może posłużyć forum przeciwdziałania przestępstwom z użyciem kart płatniczych, będące strukturą ekspercką działającą w ramach Rady Wydawców Kart Bankowych Związku Banków Polskich[10]. W nurt działań kwalifikujących się jako wymierzone w zjawisko skimmingu wpisuje się również polityka ryzyka prowadzona przez banki, polegająca na tworzeniu struktury organizacyjnej, w której skład wchodzą ogniwa odpowiedzialne za system bezpieczeństwa obrotu kartami płatniczymi, wychwytywanie, zapobieganie i wykrywanie między innymi skimmingu. Drugim elementem tych działań jest tworzenie procedur bezpieczeństwa, które warunkują działalność prewencyjną w tym zakresie. W celu zapobiegania tego typu przestępstwom banki monitorują transakcje dokonywane przez swoich klientów. Analizowane są zachowania klienta dotyczące dokonywania płatności. *Nietypowe transakcje są weryfikowane za pomocą zdefiniowanych w systemie warunków logicznych w celu zidentyfikowania transakcji nieuprawnionych (oszukańczych). Następnie wygenerowany alert jest weryfikowany przez operatora, który może podjąć określone działania, np. kontaktuje się z posiadaczem karty*[11]. W opisywanej metodzie nie mniej istotną rolę odgrywa polityka informacyjna

[10] R. Kaszubski, Ł. Obzejta, *Karty płatnicze* ..., s. 398.

[11] G. Szwajkowska, P. Kwaśniewski, K. Leżom, F. Wodniczka, *Usługi bankowości elektronicznej dla klientów detalicznych. Charakterystyka i zagrożenia*, Warszawa 2010, Urząd Komisji Nadzoru Finansowego, s. 19 i nast.

prowadzona za pośrednictwem mediów, głównie przez banki oraz organy ścigania, która ma na celu zwiększenie poziomu świadomości i wiedzy odnośnie do bezpiecznego korzystania z kart płatniczych.

Aspekty karnoprawne skimmingu

Rozpatrując problem skimmingu w świetle obowiązujących przepisów prawa karnego, należy już na wstępie podkreślić, że w *Kodeksie karnym*[12] brak jest autonomicznego uregulowania fałszerstwa karty płatniczej. Nie ma oddzielnego przepisu penalizującego przestępstwo skimmingu (fałszerstwa karty płatniczej) W praktyce nastręcza to pewnych problemów interpretacyjnych, nie wyklucza jednak represji karnej wobec sprawców tego przestępstwa. Pomimo wskazanych powyżej mankamentów, można stwierdzić, że zarówno orzecznictwo, jak i doktryna prawa karnego są w zasadzie jednolite w odniesieniu do fałszowania kart płatniczych, w tym skimmingu, co przejawia się w kwalifikowaniu powyższych czynów z art. 310 § 1 kk, tj.: *Kto podrabia albo przerabia polski albo obcy pieniądz, inny środek płatniczy albo dokument uprawniający do otrzymania sumy pieniężnej albo zawierający obowiązek wypłaty kapitału, odsetek, udziału w zyskach albo stwierdzenie uczestnictwa w spółce lub z pieniędzy innego środka płatniczego albo z takiego dokumentu usuwa oznakę umorzenia, podlega karze pozbawienia wolności na czas nie krótszy od lat 5 albo karze 25 lat pozbawienia wolności*.

Zastosowanie w przypadku sfałszowania karty płatniczej kwalifikacji z art. 310 § 1 kk jest możliwe z uwagi na zaliczenie szeroko rozumianej karty płatniczej do *innych środków płatniczych*. Prawnokarną ochroną z art. 310 § 1 kk będą objęte jedynie te środki płatnicze, które mają funkcję płatniczą. Muszą to być zatem przedmioty, którymi można się posługiwać zamiast pieniądza obiegowego, stąd nie chodzi o wszystkie walory i dokumenty traktowane i uznawane za środki płatnicze, ale jedynie takie, które podobnie jak pieniądz obiegowy mają nieograniczoną i powszechnie akceptowaną zdolność zapłaty za towar lub usługę. Podsumowując, należy stwierdzić, że środkami płatniczymi będą tylko takie walory mające funkcję płatniczą, którymi można posługiwać się w obrocie powszechnym zamiast pieniądza obiegowego, stanowiące jego ekwiwalent[13]. Warto podkreślić, że nie wszystkie typy kart płatniczych podlegają ochronie na gruncie art. 310 kk. Zaliczają się do nich karty pozbawione funkcji płatniczej, tj. przede wszystkim karty bankomatowe, gwarancyjne i konsumenckie. Powyższą tezę potwierdzają liczne orzeczenia Sądu Najwyższego i sądów powszechnych. *Karta płatnicza spełniająca funkcję płatniczą należy do zbioru desygnatów pojęcia inny środek płatniczy w rozumieniu art. 310 § 1 i 2* (wyrok SA we Wrocławiu z 20 listopada 2002 r., II AKa 467/02); ponadto Sąd Najwyższy w postanowieniu z dnia 7 października 2003 r. stwierdził, że: *karta płatnicza jako elektroniczny instrument dostępu do środków pieniężnych na odległość, umożliwiający elektroniczną identyfikację posiadacza* (…) *jest innym środkiem płatniczym* (postanowienie SN z 7 października 2003 r., V KK 39/03, Baza Orzeczeń SN). Dodatkowo w orzecznictwie ugruntował się pogląd, że karty typu *white plastic* uznaje się za podrobione karty płatnicze: *Białe karty magnetyczne z uzyskanymi i naniesionymi przez oskarżonych informacjami, będącymi drugą ścieżką oryginalnej karty płatniczej, stanowią podrobione karty płatnicze i są przedmiotem*

[12] *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny* (Dz.U. z 1997 r. Nr 88, poz. 553).

[13] *Przestępstwa przeciwko mieniu i gospodarce*, R. Zawłocki (red.), t. 9, seria: „System prawa karnego", Warszawa 2011, C.H. Beck, s. 776.

czynności wykonawczej typu czynu zabronionego z art. 310 § 1 jako inne środki płatnicze (wyrok SA we Wrocławiu z 11 lipca 2008 r., II AKa 143/08). Podobnie brzmi wyrok SA we Wrocławiu z 29 listopada 2010 r.: *Gdy zważyć na wielość i różnorodność kart płatniczych funkcjonujących w obrocie prawnym, ogromny zakres stosowania (nawet w małych placówkach handlowych) terminali POS służących realizacji zapłaty za towar, często przypadkową kadrę obsługującą stanowiska kasowe, to wygląd zewnętrzny karty płatniczej przedstawianej przez klienta ma znaczenie drugorzędne i na pewno nie może być wyznacznikiem pojęcia „karta płatnicza". Oczywiście wygląd zewnętrzny takiej karty jest zupełnie bez znaczenia w sytuacji pobierania gotówki z bankomatów. Zdatność wytworzonych przez oskarżonych (jak również innych sprawców…) „białych plastików" z naniesionymi nań danymi identyfikującymi wydawcę i posiadacza do wypłaty gotówki lub dokonywania zapłaty uprawnia do uznania, że działanie oskarżonych stanowi podrobienie innych środków płatniczych – w rozumieniu art. 310 § 1. Bez znaczenia jest – wbrew stanowisku obrońcy – czy podrobiony środek płatniczy ma wszystkie cechy oryginału. Istotne jest to, że wykonano taką jego imitację, że mogła uchodzić za oryginał, o czym świadczy fakt skutecznego posługiwania się przez oskarżonych tymi kartami na znaczną skalę, opisaną w wyroku* (wyrok SA we Wrocławiu z 29 listopada 2010 r., II AKa 325/10). Jak już wcześniej zauważono, zgodnie z poglądami wyrażonymi w doktrynie oraz orzecznictwie, poza zakresem pojęcia i n n y ś r o d e k p ł a t n i c z y pozostaje karta bankomatowa uprawniająca jedynie do pobierania gotówki z bankomatu, niemająca funkcji płatniczej. W przypadku jej sfałszowania kwalifikacja tego typu czynu nastąpi z art. 270 § 1 kk – fałszerstwo materialne dokumentu. Co więcej, karta tego typu nie może być poczytywana jako dokument uprawniający do otrzymania sumy pieniężnej z uwagi na to, że przedmiotem czynności wykonawczych czynów zabronionych określonych w art. 310 i 312 kk są wyłącznie dokumenty będące papierami wartościowymi. W związku z tym podrobienie lub przerobienie bankomatowej karty płatniczej jako „zwykłego dokumentu" podlega karnoprawnej ochronie z art. 270 § 1 kk, a nie przepisu z art. 310 § 1 kk, który to stanowi *lex specialis* w stosunku do art. 270 § 1 kk i jako przepis szczególny zapewnia ochronę dokumentom uznawanym za papiery wartościowe. Oprócz podrabiania albo przerabiania innych środków płatniczych art. 310 kk penalizuje także wiele innych zachowań przestępczych związanych z fałszowaniem kart płatniczych, co wynika z § 2: *Kto pieniądz, inny środek płatniczy lub dokument określony w § 1 puszcza w obieg albo go w takim celu przyjmuje, przechowuje, przewozi, przenosi, przesyła albo pomaga do jego zbycia lub ukrycia, podlega karze pozbawienia wolności od roku do lat 10*. Z uwagi na charakter dóbr prawnych, które są przedmiotem ochrony tego artykułu, ustawodawca przewidział karalność przygotowania do przestępstwa określonego zarówno w § 1, jak i w § 2 art. 310 kk. Jak słusznie zauważyła R. Kędziora: *Art. 310 § 4 kk daje w szczególności możliwość postawienia zarzutu przygotowania do fałszerstwa osobie, u której w posiadaniu znajdują się zapisy zawartości pasków magnetycznych czy czyste białe karty, tzw. biały plastik. Przepis ten znajduje więc zastosowanie także do czynności przygotowawczych do fałszowania metodą białego plastiku*[14]. Jeśli chodzi o dokonywanie oszukańczych transakcji za pomocą sfałszowanej karty, to w grę będzie wchodziła kwalifikacja tego typu zachowań z dwóch artykułów kodeksu karnego, tj. art. 286 kk lub art. 287 kk. W przypadku gdy sprawca, posługując się sfałszowaną kartą, wprowadzi w błąd inną osobę lub wyzyska jej błędne przekonanie, że jest on

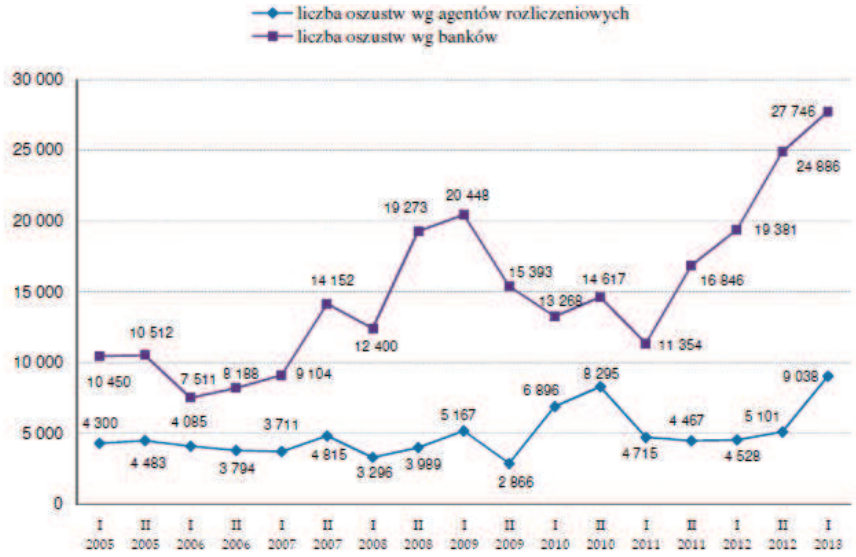
[14] R. Kędziora, *Przestępstwa z wykorzystaniem kart płatniczych – aspekty karnoprawne*, w: *Wyzwania w systemie bankowym w XXI w.*, A. Piotrowska-Piątek, P. Ruczkowski (red.), Kielce 2009, WSEIP Kielce, s. 376.

osobą uprawnioną do posługiwania się tą kartą, to tego typu zachowanie należy rozpatrywać w kategoriach oszustwa z art. 286 § 1 kk. Cechą charakterystyczną dla tej sytuacji będzie kontakt z drugą osobą, a więc posługiwanie się sfałszowaną kartą w punkcie usługowo-handlowym. W sytuacji zaś, gdy sprawca użyje takiej karty do dokonania wypłaty gotówki z bankomatu, nie można mówić o wprowadzeniu w błąd drugiej osoby, co jest niezbędne do przyjęcia kwalifikacji z art. 286 § 1 kk. W tym przypadku w grę wejdzie kwalifikacja z art. 287 kk, gdyż działanie sprawcy przejawia się wpływaniem bez upoważnienia na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych w celu osiągnięcia korzyści majątkowej. Z tego przepisu będzie więc odpowiadać karnie sprawca wypłacający pieniądze z bankomatu za pomocą m.in. sfałszowanej karty, ponieważ tego typu działanie prowadzi do zmniejszenia sumy środków pieniężnych na rachunku bankowym posiadacza poprzez wpływ na automatyczne przetwarzanie informacji, jakimi są dane o stanie tegoż rachunku. Rozpatrując wszystkie zachowania przestępcze sprawcy składające się na skimming, należy podkreślić, że zarówno w praktyce orzeczniczej sądów, jak i w doktrynie stosowana jest kumulatywna kwalifikacja prawna, przybierająca w zależności od wyżej opisanych różnic następujące formy: art. 310 § 1 kk w zb. z art. 286 § 1 kk w zw. z art. 11 § 2 kk lub art. 310 § 1 kk w zb. z art. 287 § 1 kk w zw. z art. 11 § 2 kk, ewentualnie wzbogaconych o art. 12 kk. W zależności od stanu faktycznego konkretnej sprawy może zaistnieć rzeczywisty zbieg przepisów art. 310 § 1 kk i art. 310 § 2 kk, a nawet realny lub pozorny zbieg przestępstw, których znamiona wyczerpują oba przepisy kodeksu karnego.

W doktrynie można również natrafić na propozycję odmiennej kwalifikacji posługiwania się sfałszowaną kartą płatniczą, która przyjmuje, że posłużenie się taką kartą do dokonania transakcji płatniczej można poczytywać za *puszczenie karty płatniczej w obieg*, co skutkuje subsumpcją opisanego zachowania pod normę prawną wyrażoną w art. 310 § 2 kk[15].

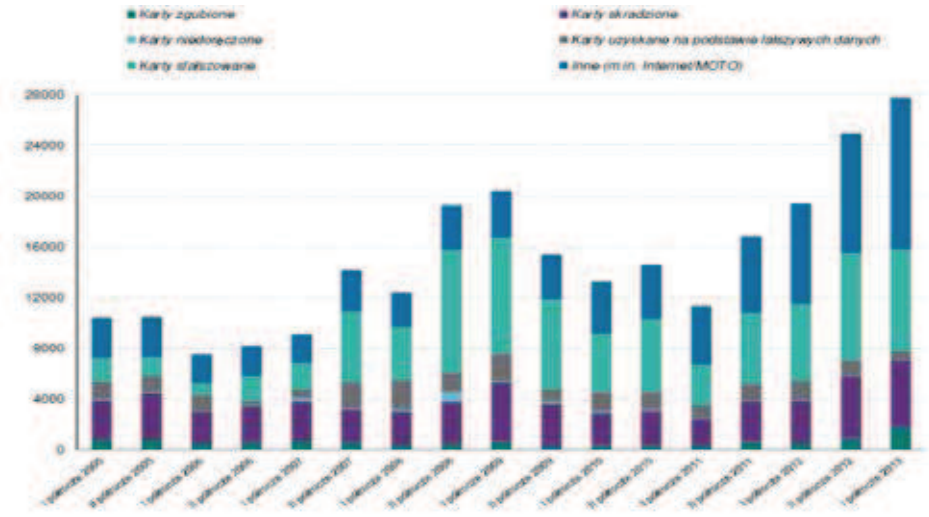
[15] R. Kaszubski, Ł.Obzejta, *Karty płatnicze...*, s. 418.

Dane statystyczne



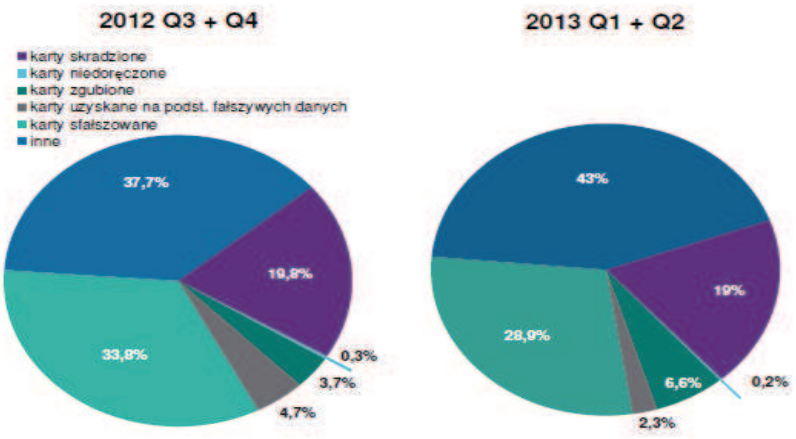
Wykres 1. Liczba oszustw według banków i agentów rozliczeniowych w latach 2005–2013.

Źródło: *Ocena funkcjonowania polskiego systemu płatniczego w I półroczu 2013 roku,* Warszawa 2013, Departament Systemu Płatniczego NBP.



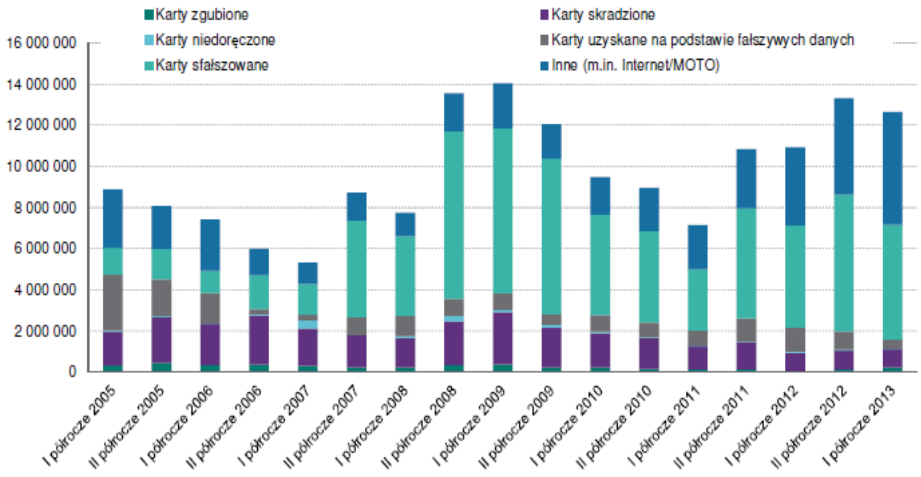
Wykres 2. Liczba operacji oszukańczych z wykorzystaniem kart płatniczych w poszczególnych półroczach w latach 2005–2013 w podziale na rodzaje operacji oszukańczych – dane od banków.

Źródło: *Ocena funkcjonowania polskiego systemu płatniczego w I półroczu 2013 roku,* Warszawa 2013, Departament Systemu Płatniczego NBP.



Wykres 3. Struktura operacji oszukańczych kartami płatniczymi według liczby w II półroczu 2012 r. i w I półroczu 2013 r.

Źródło: *Ocena funkcjonowania polskiego systemu płatniczego w I półroczu 2013 roku,* Warszawa 2013, Departament Systemu Płatniczego NBP.



Wykres 4. Wartość operacji oszukańczych z wykorzystaniem kart płatniczych w poszczególnych półroczach w latach 2005–2013 (w polskich złotych) – podział na rodzaje operacji oszukańczych.

Źródło: *Ocena funkcjonowania polskiego systemu płatniczego w I półroczu 2013 roku,* Warszawa 2013, Departament Systemu Płatniczego NBP.

Bibliografia:

Literatura:

Błachut J., *Dokument jako przedmiot ochrony prawnokarnej*, Warszawa 2011, Wolters Kluwer S.A.

Kaszubski R., Obzejta Ł., *Karty płatnicze w Polsce,* Warszawa 2012, Wolters Kluwer S.A.

Kędziora R., *Przestępstwa z wykorzystaniem kart płatniczych – aspekty karnoprawne*, w: *Wyzwania w systemie bankowym w XXI w.*, A. Piotrowska-Piątek, P. Ruczkowski (red.), Kielce 2009, Wydawnictwo WSEiP Kielce.

Kodeks karny. Część szczególna, Tom II, *Komentarz do artykułów 222–316*, A. Wąsek, R. Zawłocki (red.), Warszawa 2010, C.H. Beck.

Kodeks karny. Część szczególna, Tom II, Komentarz do artykułów 222–316, M. Królikowski, R. Zawłocki (red.), seria: „Duże komentarze Becka", Warszawa 2013, C.H. Beck.

Kodeks karny. Część szczególna. Tom III, Komentarz do art. 278–363, A. Zoll (red.), Warszawa 2008, Wolters Kluwer S.A.

Kodeks karny. Praktyczny komentarz, M. Mozgwa (red.), Warszawa 2010, Wolters Kluwer S.A.

Marek A., *Kodeks karny. Komentarz*, Warszawa 2005, ABC.

Ocena funkcjonowania polskiego systemu płatniczego w I półroczu 2013 roku, Warszawa 2013, Departament Systemu Płatniczego NBP.

Podsiedlik P., Czylok T., *Przestępczość w bankowości elektronicznej*, Katowice 2010, Wydawnictwo WSP w Katowicach.

Przestępstwa przeciwko mieniu i gospodarce, R. Zawłocki (red.), t. 9, seria: „System prawa karnego", Warszawa 2011, C.H. Beck.

Stefański R.A., *Prawo karne materialne. Część szczególna*, Warszawa 2009, Difin.

Szwajkowska G., Kwaśniewski P., Leżom K., Wodniczka F., *Usługi bankowości elektronicznej dla klientów detalicznych. Charakterystyka i zagrożenia*, Warszawa 2010, Urząd Komisji Nadzoru Finansowego.

Wyrok SA we Wrocławiu z dnia 11 lipca 2008 r., II AKa 143/08, „Biuletyn Sądu Apelacyjnego we Wrocławiu" 2009, nr 3 (11), s. 16.

Zajda M., *Prawno-kryminalistyczne aspekty przestępczości z użyciem elektronicznych instrumentów płatniczych*, Słupsk 2003, Wydawnictwo Szkoły Policji w Słupsku.

Akty prawne:

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, Dz.U. z 1997 r. Nr 88, poz. 553.

Abstrakt

Niniejszy artykuł dotyczy skimmingu będącego stosunkowo nowym i ciągle ewoluującym rodzajem przestępstwa zarówno w Polsce, jak i za granicą. Autor podjął próbę przybliżenia tego ustawowo niezdefiniowanego w prawie karnym przestępstwa, wskazując jednocześnie na jego cechy charakterystyczne, elementy składowe, a także na modus operandi jego sprawców. Oprócz omówienia rodzajów skimmingu, zagadnień technicznych z nim związanych oraz skutków tego typu przestępstwa, artykuł zawiera

również charakterystykę wielopłaszczyznowej polityki zwalczania opisywanego zjawiska. Autor nakreślił także ogólny zarys praktyki orzeczniczej i zapatrywań doktryny odnoszący się do skimmingu.

Abstract

The article treats of skimming phenomenon, which is a relatively new and continuously evolving criminal method both in the national and international environment. Author of this article tries to describe this term, which is an offence unidentified in the criminal law, and simultaneously he demonstrates its characteristics, component parts and modus operandi of perpetrators. Apart from describing different types of skimming, technical issues linked with it and results of this type of crime, this study also contains characteristics of multidimensional policy of combating this phenomenon. Furthermore, author ventured to provide general outline of judicial practice and doctrine's outlook on skimming.