DANIEL M. ZAWADKA*

WSPÓŁCZESNA PRZESTĘPCZOŚĆ ZWIĄZANA Z PIENIĄDZEM ELEKTRONICZNYM. ROLA ORGANÓW ŚCIGANIA

Abstrakt

Działania przestępcze wymierzone w legalnych posiadaczy kart płatniczych dalej utrzymują się na wysokim poziomie. Powszechność dokonywania płatności kartą sprawia, że przestępcy dalej sięgają do narzędzi jakimi są skimmery oraz uciekają się do ataków phishingowych z wykorzystaniem socjotechniki, licząc na naiwność swoich potencjalnych ofiar. Płatności elektroniczne są ponadto dla przestępców jedną z częściej wybieranych form „prania pieniędzy". Wobec tak powszechnej i rozwiniętej gałęzi przestępczości, obojętne nie pozostają organy ścigania, dążąc do podnoszenia poziomu wykrywalności sprawców.

Słowa kluczowe: pieniądz elektroniczny, skimming, phishing, carding.

Przestępczość w sektorze płatności bezgotówkowych i akceptacji kart płatniczych stanowi w ostatnich latach znaczny odsetek wśród przestępstw związanych z kradzieżą, finansami i szeroko pojętą przestępczością gospodarczą, oraz zorganizowaną. Na tę sytuację istotne przełożenie ma postępujący proces dematerializacji pieniądza, oraz powszechność dokonywania rozliczeń finansowych i zapłat za produkty bądź usługi za pośrednictwem karty płatniczej lub poprzez inne formy elektronicznego dostępu do rachunku bankowego. Za sprawą postępu technologicznego elektroniczna rewolucja obiegu pieniądza dotyczy już praktycznie każdego. Nowoczesne formy kontaktu z bankiem drogą elektroniczną, stały się już standardem, w wyniku czego te tradycyjne siedziby i placówki banków spychane są na margines uzupełniania bankowości internetowej[1]. Pomijając te najstarsze formy bezgotówkowych płatności, za jakie możemy uznać polecenia przelewu, polecenia zapłaty, czeki

* Daniel M. Zawadka – student studiów magisterskich bezpieczeństwa wewnętrznego na UTH im. Heleny Chodkowskiej w Warszawie. W przeszłości związany z sektorem akceptacji kart płatniczych, współpracował z czołowymi acquirerami na polskim rynku. Kontakt e-mail: daniel.zawadka@uth.pl

[1] A. Prokopiuk, *Wybrane aspekty rozwoju e-bankowości w Polsce*, [w:] T. Mikulska, J. Sikorski (red.), *Stan i perspektywy rozwoju współczesnej bankowości*, Białystok 2014, s. 145.

rozrachunkowe, weksle[2] czy nawet przelewy internetowe, a skupiając się stricte na akceptacji kart płatniczych, właściwym wydaje się stwierdzenie, że opanowały one niemalże wszystkie gałęzie branży handlowo-usługowej. Kartą możemy zapłacić prawie wszędzie, nie tylko w standardowym sklepie stacjonarnym, ale również przez Internet, czy w różnego rodzaju urządzeniach samoobsługowych. Akceptacja kart płatniczych jest możliwa w biletomatach komunikacji miejskiej, czy na dworcach kolejowych, które umożliwiają pasażerom bezpieczną formę płatności zbliżeniowej, zwanej również bezstykową, opartą na technologii NFC, opartą na radiokomunikacji krótkiego zasięgu na pasmie wysokich częstotliwości, która pozwala na szybką wymianę danych pomiędzy kartą a czytnikiem na odległość do kilku centymetrów[3]. Tego typu czytniki zbliżeniowe są bardzo powszechnie stosowane zarówno w biletomatach jak i w automatach vendingowych oferujących kawę, zimne napoje, czy przekąski, parkomatach, czy chociażby na stacjach warszawskiego systemu rowerów miejskich Veturilo.

Z uwagi na przedstawioną wyżej wygodę, mobilność i powszechność występowania czytników kart płatniczych w niemalże każdej gałęzi branży handlowo-usługowej, a także szybkość dokonywania transakcji, oraz bezpieczeństwo wynikające z braku konieczności noszenia przy sobie gotówki przez społeczeństwo, sposób działania przestępców czyhających na szanse okradzenia innych obywateli naturalnie uległ zmianie. Aktualne modus operandi sprawców uwzględnia przede wszystkim uzyskiwanie nieuprawnionego elektronicznego dostępu do środków zgromadzonych na kontach swoich ofiar, natomiast typologia przestępczości tego typu z uwagi na rozległość przedmiotową i zróżnicowanie form dysponowania pieniądzem elektronicznym, jest zagadnieniem dosyć obszernym, które w dodatku ulega ciągłym przekształceniom z racji wdrażanych zabezpieczeń technologicznych ze strony środowisk bankowych i organizacji płatniczych. Podobnie wygląda kwestia dostosowania do ewoluującej przestępczości, metodyki czynności podejmowanych przez środowiska bankowe i organy ścigania. Zauważalny jest również wzrost świadomości samych posiadaczy kart w kwestii bezpieczeństwa posługiwania się instrumentami, jakie daje im bankowość elektroniczna, lecz mimo tego według banków oraz organów ścigania to ciągle człowiek jest najsłabszym ogniwem, szczególnie wobec stosowanej przez przestępców socjotechniki w kontekście wyłudzania danych umożliwiających elektroniczny dostęp do pieniędzy zgromadzonych koncie bankowym.

Definicja pieniądza elektronicznego

Treść ustawy o usługach płatniczych[4] rozdziela pojęcia instrumentu płatniczego definiowanego jako zindywidualizowane urządzenie lub uzgodniony przez użytkownika i dostawcę zbiór procedur, wykorzystywane przez użytkownika do złożenia zlecenia płatniczego. A także odrębne pojęcie pieniądza elektronicznego, określonego jako wartość pienięż-

2 S. Flajterski, B. Świecka, *Elementy finansów i bankowości*, Warszawa 2007, s. 265–266.

3 A. Grzybowska, *Innowacyjne rozwiązania na rynku usług płatniczych*, [w:] T. Mikulska, J. Sikorski (red.), *Stan i perspektywy rozwoju współczesnej bankowości*, Białystok 2014, s. 115.

4 Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych, tekst jednolity Dz.U. 2016 poz. 1572.

ną przechowywaną elektronicznie, w tym magnetycznie, wydawaną, z obowiązkiem jej wykupu, w celu dokonywania transakcji płatniczych, akceptowaną przez podmioty inne niż wyłącznie wydawca pieniądza elektronicznego[5]. Wcześniej na obszarze Unii Europejskiej również wprowadzono mocą stosownej dyrektywy[6] pojęcie pieniądza elektronicznego. Jej znowelizowana wersja opracowana przez Parlament Europejski i Radę, zastępująca poprzednią w roku 2009, określa pieniądz elektroniczny jako wartość pieniężną przechowywaną elektronicznie, w tym magnetycznie, stanowiącą prawo do roszczenia wobec emitenta, która jest emitowana w zamian za środki pieniężne w celu dokonywania transakcji płatniczych i akceptowana przez osoby fizyczne lub prawne inne niż emitent pieniądza elektronicznego[7]. Dodatkowo w literaturze można spotkać się z dwiema postaciami pieniądza elektronicznego, określonego jako:

- produkt bazujący o technologię kart procesorowych, tzw. elektroniczną portmonetkę (z ang. *electronicpurse, multipurpose prepaid card*),
- produkt wykorzystujący oprogramowanie, przy pomocy którego posiadacz może dokonać płatności w Internecie, tzw. pieniądz sieciowy (z ang. *network based, software basedproduct*)[8].

Wydawanie instrumentu pieniądza elektronicznego jest natomiast czynnością bankową *sensu stricto*[9].

Skimming – najpowszechniejsze przestępstwo godzące w legalnych posiadaczy kart płatniczych

Postęp technologiczny wymusił szereg zmian również na przestępcach, którzy z kradzieży tradycyjnych portfeli, przekierowali swoje zainteresowanie na elektroniczne portmonetki, jakimi są karty płatnicze. Według ustawy o usługach płatniczych, kartą płatniczą nazywamy kartę uprawniającą do wypłaty gotówki lub umożliwiającą złożenie zlecenia płatniczego za pośrednictwem akceptanta lub agenta rozliczeniowego, akceptowaną przez akceptanta w celu otrzymania przez niego należnych mu środków[10]. W literaturze polskojęzycznej nie ma jednego wspólnego określenia co do charakteru prawnego karty płatniczej. Podkreślany jest jednak fakt, że karta nie jest nową typową formą pieniądza bezgotów-

5 Tamże, s. 4–6.

6 Dyrektywa 2000/46/EC Parlamentu Europejskiego i Rady z dnia 18 września 2000 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalności, Dz. U. L 275/39 z 21 października 2000 r.

7 Dyrektywa 2009/110/WE Parlamentu Europejskiego i Rady z dnia 16 września 2009 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością, zmieniająca dyrektywy 2005/60/WE i 2006/48/WE oraz uchylająca dyrektywę 2000/46/WE, Dz. U. L 267/7 z 10 października 2009 r.

8 R. Janowicz, *Pieniądz elektroniczny na świecie*, [w:] J. Kosiński (red.), *Przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych*, Szczytno 2003, s. 21.

9 A. Mikos-Sitek, P. Zapadka, *Polskie prawo bankowe. Wybrane zagadnienia*, Warszawa 2011, s. 178.

10 Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych, tekst jednolity Dz.U. 2016 poz. 1572.

kowego, gdyż posiadacz dysponuje środkami zgromadzonymi na rachunku bankowym[11], tylko raczej jako klucz dostępu[12], lub instrument dostępu do środków zgromadzonych na rachunku bankowym, za pomocą którego możliwa jest wypłata gotówki z bankomatu lub dokonywanie zapłaty[13].

Skimming jest bezprawnym skopiowaniem informacji zapisanych na pasku magnetycznym karty, oraz przechwyceniem kodu PIN (niezbędnego do autoryzacji transakcji na szkodę legalnego posiadacza karty), bez wiedzy i zgody posiadacza, w celu sfałszowania karty przez wykonanie jej fizycznego duplikatu, mającego posłużyć do przestępczego obciążenia rachunku bankowego prawowitego posiadacza karty[14]. Informacja zapisana na pasku magnetycznym, która jest dla przestępców interesująca, zawarta jest w praktyce na dwóch z trzech ścieżek paska magnetycznego karty. Zawartość ścieżek paska magnetycznego karty określa norma ISO-7811. Pierwsza z nich, alfanumeryczna zawiera dane posiadacza karty, czyli imię, nazwisko, numer karty, oraz informacje dodatkowe jakimi są: data ważności, zastrzeżenia lub typ, a także kod CVV/CVC2. Druga z nich, typowo numeryczna zawiera powtórzony numer karty i informacje dodatkowe[15]. Forma zapisu danych na pasku magnetycznym karty płatniczej pod względem technologicznym nie różni się od poziomu skomplikowania zapisu danych na dyskietce, czy kasecie magnetofonowej. Przy użyciu urządzeń stosunkowo niedrogich i dostępnych w przestępczym półświatku, a także dzięki dobrodziejstwu medium jakim jest Internet, wraz z całym zgromadzonym w sieci zasobem porad i koncepcji skutecznego kopiowania zawartości kart i ich fałszowania, przestępcze *know-how* jest aktualnie dostępne dla każdego obywatela – internauty, rozważającego zboczenie z drogi uczciwej egzystencji w społeczeństwie. Popyt potencjalnych sprawców na coraz to bardziej zminimalizowane i pasujące (np. do elementów bankomatów) skimmery, jest istotnym czynnikiem dalszego i trwałego rozwoju produkcji narzędzi przestępstwa tego typu.

Zjawisko skimmingu możemy dodatkowo podzielić na dwie kategorie, z uwagi na miejsce oraz urządzenie z wykorzystaniem którego sprawca dopuszcza się przestępstwa odczytania danych zapisanych na karcie płatniczej. Pierwszą z nich jest skimming w punkcie handlowo-usługowym, który polega na zeskanowaniu informacji z paska magnetycznego karty płatniczej w momencie dokonywania płatności, najczęściej przez nieuczciwego sprzedawcę lub pracownika[16]. Do tego rodzaju procederu używa się np. miniaturowych, mieszczących się w dłoni skimmerów wyposażonych w baterię oraz wbudowaną pamięć zdolną pomieścić określoną ilość danych. Rozmiar urządzenia ma w tym przypadku znaczenie, jeśli sprawca stojąc w pobliżu prawnego posiadacza karty, sczytuje z niej dane w sposób niezauważalny dla klienta, wykorzystując urządzenie trzymane w dłoni, lub zamocowane przy kasie pod blatem. Poza odczytaniem zawartości paska magnetycznego, sprawcom

---

11 M. Pacak, *Ustawa o elektronicznych instrumentach płatniczych. Komentarz*, Warszawa 2013, s. 64.

12 A. Michór, *Kartypłatnicze*, [w:] W. Góralczyk (red.), *Problemy współczesnej bankowości. Zagadnienia prawne*, Warszawa 2014, s. 265.

13 A. Mikos-Sitek, P. Zapadka, dz. cyt., s. 178.

14 K. Mikołajczyk, *Przestępstwa związane z wykorzystywaniem bankowości elektronicznej – skimming*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 10(6), s. 104.

15 J. Kosiński, *Paradygmaty cyberprzestępczości*, Warszawa 2015, s. 160.

16 B. Kowalski, *Problematyka przestępstw dotyczących kart płatniczych na przykładzie skimmingu i cardingu*, „Przegląd Policyjny" 2015, Nr 4(120), s. 170.

potrzebny jest jeszcze kod PIN, który mogą osobiście podejrzeć w momencie wpisywania go przez klienta – posiadacza karty, na klawiaturze terminala płatniczego, lub PinPada podłączonego do terminala, a także poprzez nakierowanie monitoringu w lokalu na klawiaturę służącą do wpisywania PIN-u. Drugą z form skimmingu jest bankomatowa odmiana tego przestępstwa. Polega ona na nielegalnej modyfikacji budowy bankomatu ATM, mającej na celu zamontowanie urządzenia służącego do kopiowania danych z paska magnetycznego karty[17]. Skimmery przymocowuje się w miejscu slotu-gniazda do którego wkładamy kartę w bankomacie aby pobrać z niego gotówkę (lub ją wpłacić jeśli mamy do czynienia z urządzeniem z funkcją wpłatomatu). Najczęściej przybierają one formę nakładki komponującej się z obudową, lub są dokładną repliką elementu obudowy. Poza skopiowaniem zawartości paska magnetycznego, przestępcy muszą ponadto uzyskać kod PIN niezbędny do pełnego wykorzystania potencjalnej sklonowanej karty. W tym celu wykorzystują dopasowane nakładki na klawiaturę bankomatu, które poprzez umiejscowienie tuż nad właściwą klawiaturą „przekazują" do bankomatu kod PIN oraz komendy zatwierdzane na klawiaturze przez nieświadomego przestępczego procederu posiadacza karty. Ponadto rejestrują wpisywane cyfry, albo zapisując je na module pamięci opartej najczęściej na kartach SD lub microSD, albo bezpośrednio przesyłając je drogą radiową do komputera, lub innego urządzenia znajdującego się w zasięgu – najczęściej w samochodzie zaparkowanym niedaleko bankomatu ATM. Dane mogą być również przesyłane bezpośrednio na drugi koniec świata za pomocą modułu łączności GPRS opartego na karcie SIM, wykorzystującej transmisje danych internetowych. Istotne w urządzeniu jest również alternatywne źródło zasilania, najczęściej w postaci baterii lub miniaturowego akumulatora.

Inną z form uzyskiwania kodu PIN przez sprawców skimmingu jest instalowanie miniaturowej kamery skierowanej na klawiaturę bankomatu. W tej sferze pomysłowość przestępców również nie zna granic. Wykorzystują oni różnego rodzaju doczepiane listwy reklamowe, wypukłe naklejki z logotypami, czy nawet doczepiane do bankomatów pojemniki na ulotki z ofertą banku[18]. Zminiaturyzowane urządzenie charakteryzujące się wydajnością w przestępczym procederze powinno być w stanie rejestrować obraz przez kilka lub kilkanaście godzin, co wymusza na konstruktorach wykorzystanie miniaturowego lecz pojemnego nośnika pamięci, oraz kolejnego alternatywnego źródła zasilania w postaci baterii lub niewielkiego akumulatora. Wyższym poziomem zaawansowania technologicznego wśród metod uzyskiwania kodu PIN wyróżniają się przestępcy, którzy opanowali dodatkowo technologię przechwytywania numeru z sygnału elektromagnetycznego oraz wykorzystywania śladu termicznego palców ofiary z klawiatury bankomatu[19]. Zjawisko skimmingu z uwagi na potencjalny większy zysk sprawców, najczęściej dotyka bankomaty w dobrych lokalizacjach turystycznych, oraz te niezlokalizowane w oddziałach bankowych, do których jest swobodny dostęp i z których korzysta duża liczba osób, gdyż w takich miejscach nikogo nie dziwią ślady zużycia mechanicznego na bankomacie, które mogłyby wskazywać na próby modyfikowania obudowy bankomatu, lub inną podejrzaną działal-

17 Tamże, s. 168.

18 J. Gąsiorowski, P. Podsiedlik, *Przestępstwa w bankowości elektronicznej w Polsce. Próba oceny z perspektywy prawno-kryminalistycznej*, Dąbrowa Górnicza 2015, s. 112.

19 J. Kosiński, dz. cyt., s. 159.

ność, ani fakt, że w większych miastach lub obiektach turystycznych w pobliżu bankomatu ciągle znajdują się ludzie[20].

Skimming jest przestępstwem charakterystycznym z uwagi na swój międzynarodowy wymiar. Z racji wyższego poziomu zabezpieczeń przyjętych przez organizacje płatnicze z jakim mamy do czynienia w Europie, w porównaniu z zarówno Ameryką Północną jak i Południową, na co ogromny wpływ ma wprowadzony tzw. standard EMV, finalizowanie przestępczego procederu w postaci wypłacania pieniędzy z kont Polaków czy ogólnie Europejczyków, ma miejsce na terenie obu Ameryk, gdzie zabezpieczenia bankowe są na znacznie gorszym poziomie, a udział w rynku kart z mikroprocesorem jest niestety w dalszym ciągu znikomy. W ciągu ostatnich lat większość nielegalnych wypłat środków z kont naszych obywateli w oparciu o sfałszowane karty płatnicze, miała miejsce głównie w Ameryce Południowej[21]. Analizując doniesienia prasowe i kroniki policyjne, nietrudno zauważyć, że na terenie Polski w związku ze skimmingiem najczęściej zarzuty stawiane są obywatelom Mołdawii, Bułgarii i Rumunii[22], którzy prowadzą u nas zorganizowaną działalność przestępczą. Atrakcyjność Polski jako terytorium działania zorganizowanych grup przestępczych z udziałem cudzoziemców wynika głównie z postrzegania RP jako kraju bezpiecznego, stabilnego i rozwiniętego ekonomicznie, którego gospodarka posiada duży potencjał rozwoju, a co za tym idzie możliwości jej nielegalnej eksploatacji. Do tego dochodzi fakt członkostwa w UE i strefie Schengen oraz centralnego położenia w Europie na trasie szlaków komunikacyjnych łączących wschód z zachodem kontynentu[23].

Phishing

Phishing jest rodzajem oszustwa internetowego, które ma na celu kradzież tożsamości, czyli poufnych danych osobistych, np. numerów kart kredytowych, haseł do systemów bankowych, czy haseł do portali oferujących aukcje internetowe. Termin ten pochodzi z języka angielskiego od sformułowania *password hervesting fishing*, oznaczającego łowienie haseł. Samo przestępstwo polega na nakłonieniu użytkownika do samodzielnego wpisania poufnych danych na specjalnie przygotowanej stronie internetowej, mającej imitować oryginalną stronę instytucji (np. banku internetowego, serwisu aukcyjnego, czy internetowego serwisu płatności), pod którą podszywają się oszuści[24]. Sprawcy najczęściej wysyłają do ofiar spreparowane listy elektroniczne, pochodzące rzekomo z banku, wymuszając na poszkodowanym natychmiastowy kontakt drogą elektroniczną pod legendą odblokowania konta, weryfikacji danych karty dla przedłużenia jej ważności, ponownej jej aktywacji, dodania nowej aplikacji, czy poprawy procedur bezpieczeństwa dokonywanych transak-

20 B. Kowalski, dz. cyt., s. 169.

21 *Kradzież w Polsce, wypłata w Peru*, „Rzeczpospolita" z dn. 12.01.2015 r.

22 *Nie zawsze warto kartą*, „Dziennik Trybuna" z dn. 11.02.2015 r.

23 K. Laskowska, *Działalność zorganizowanych grup przestępczych z udziałem cudzoziemców w Polsce w latach 2004–2013 w świetle policyjnych badań statystycznych*, „Przegląd Policyjny" 2016, nr 3(123), s. 18.

24 R. Wilczewski, *Phishing – popełnianie i zwalczanie*, [w:] J. Kosiński, S. Kmiotek (red.), *Przestępczość teleinformatyczna*, Szczytno 2011, s. 258.

cji[25]. Charakteryzując zjawisko przestępczości w bankowości elektronicznej na przykładzie phishingu, nie sposób nie wspomnieć o tworzonym przez cyberprzestępców złośliwym oprogramowaniu, które uważane jest za jedno największych zagrożeń dla bankowości elektronicznej. Poprzez złośliwe oprogramowanie cyberprzestępcy próbują pozyskać nasze środki finansowe lub tylko dane, które są potrzebne do pozyskania tychże środków. Poza trojanami Rbot, Sinowal czy Limbo2, popularnymi kilkanaście lat temu, na polskim rynku bankowym spustoszenie swego czasu siał trojan nazywany Zeus lub Zbot, który modyfikował transakcje elektroniczne poprzez podmienienie numeru rachunku odbiorcy oraz wysokości kwoty. Zmodyfikowana wersja Zeusa była dodatkowo w stanie podmienić stronę bankową generując prośbę o podanie pełnego hasła, a także wyłudzała dane telefonu klienta, służącego do odbierania kodów autoryzacyjnych, infekowała telefon klienta banku złośliwym oprogramowaniem, a w efekcie finalnym dokonywała transakcje w imieniu klienta. W ostatnich latach również zarejestrowano w Polsce przypadki ataków socjotechnicznych z wykorzystaniem trojana Zeus w wersjach Citadel i 2P2, inspirujących klienta do wykonania rzekomo testowej transakcji, wyłudzając tym sposobem dane logowania i środki finansowe przez naiwność internautów. Natomiast za wschodnią granicą naszego kraju zdarzały się przypadki instalowania trojanów w bankomatach poprzez nawiercenie obudowy w miejscu wewnętrznego gniazda USB i podpięcie pendriva z automatycznie instalującym się złośliwym oprogramowaniem, które rejestrowało i umożliwiało przestępcom pozyskanie wpisywanego kodu PIN oraz danych z drugiej ścieżki paska magnetycznego karty płatniczej[26].

Autorzy publikacji z dziedziny cyberprzestępczości wskazują również na możliwość pozyskiwania danych o kartach płatniczych z terminali POS, poprzez odpowiednio spreparowane oprogramowanie i przesyłanie danych na pomocą różnych form łączności – np. bluetooth lub Wi-Fi, lub zapisywania ich we wmontowaną nielegalnie w POS wymienną kartę pamięci[27]. Jednakże z uwagi na technologiczny wymiar skomplikowanej aplikacji obsługującej płatności w terminalu oraz nadzoru jej przez systemy TMS należące do acquirerów lub kooperujących z nimi podmiotów, jest to raczej trudny a z pewnością szerzej nieznany wymiar przestępczości terminalowej, w który swój wkład teoretycznie musiałby mieć akceptant jakim jest przedsiębiorca dzierżawiący terminal płatniczy.

Cyberlaundering – „pranie pieniędzy" za pośrednictwem pieniądza elektronicznego

Pojawienie się nowych technologii umożliwiających dokonywanie natychmiastowych transferów pieniężnych, może przełożyć się na ułatwienie zadania przestępcom w procederze prania pieniędzy[28]. Efektem tego katalog legalizacji środków pochodzących z prze-

[25] J. Gąsiorowski, P. Podsiedlik, dz. cyt., s. 147.

[26] P. Olszar, *Złośliwe oprogramowanie w bankowości elektronicznej*, [w:] J. Kosiński (red.), *Przestępczość teleinformatyczna*, Szczytno 2013, s. 307–316.

[27] J. Kosiński, dz. cyt., s. 162.

[28] D. Cyman, *Elektroniczne instrumenty płatnicze a bezpieczeństwo użytkowników rynku finansowego*, Warszawa 2013, s. 245.

stępstw wzbogacił się o pojęcie *cyberlaunderingu* – wygodnej i bezpiecznej legalizacji z wykorzystaniem transakcji elektronicznych, dokonywanej najczęściej przez sieć internetową. D. Cyman wśród popularnych elektronicznych instrumentów płatniczych wskazuje na wykorzystywanie systemu kart przedpłaconych, które z uwagi na swoją anonimowość są idealną formą transgranicznego transferu środków pieniężnych, w szczególności z wykorzystaniem kart wydawanych w rajach podatkowych, gdzie obowiązują rygorystyczne regulacje dotyczące tajemnicy bankowej[29].

Jerzy Kosiński w kontekście prania pieniędzy w wymiarze cyberprzestępczości, a co za tym idzie wykorzystaniu elektronicznych instrumentów płatniczych, wymienia trzy formy legalizacji środków finansowych pochodzących z przestępstwa, jakimi są:

- *moneymulles* – rekrutowani na niszowych portalach oferujących pracę, która polega na dokonywaniu transferu otrzymywanych od przestępców kwot na wskazane konta bankowe, w zamian za ustaloną kwotę prowizji. W tym procederze konta praczy zakłada się w bankach, których klienci mają być ofiarami dokonywanych przestępstw finansowych, co pozwala na szybki transfer pieniędzy pomiędzy rachunkami w tym samym banku;
- internetowe gry on-line o charakterze MMORPG, w których internetowi gracze korzystają z wirtualnych kredytów wykupowanych i wymienialnych na realne pieniądze. Przy użyciu wielu kont, łączących graczy z wielu krajów możliwe jest szybkie wprowadzenie, transfer międzynarodowy, oraz powrót do wpłacającego lub wypłata środków poza granicami;
- mikropralnie polegające na wykorzystywaniu usług podobnych do PayPal w połączeniu z płatnościami mobilnymi i tradycyjnymi usługami płatniczymi, poprzez przenoszenie pieniędzy różnymi środkami transferowania w postaci niewielkich kwot przelewanych z dużą częstotliwością, co utrudnia powstrzymywanie prania brudnych pieniędzy[30].

Działania podejmowane przez organy ścigania

Bezpieczeństwo prawne transakcji jest zespołem regulacji prawnych wyznaczających określone zachowania, które mają być podejmowane przez osoby i instytucje, których dotyczą te przepisy[31]. W przypadku stwierdzenia odstępstw od wyznaczonych zachowań, uzyskanych w ramach zgłoszenia osoby poszkodowanej, instytucji finansowej, organizacji płatniczej, czy zauważenia tego podczas prowadzenia postepowania w innej sprawie, lub w wyniku podejmowanych czynności operacyjno-rozpoznawczych, reagują na to uprawnione organy ścigania, wszczynając postepowanie przygotowawcze[32].

---

29 Tamże, s. 246.

30 J. Kosiński, dz. cyt., s. 156.

31 *Bezpieczeństwo prawne transakcji dokonywanych kartami płatniczymi*, „Gazeta Prawna" z dn. 11.12.2008 r.

32 Z uwagi na właściwości wynikające z ustaw szczególnych, a także z k.p.k., do realizacji czynności procesowych w związku z przestępczością kartową właściwa jest Policja, lub Żandarmeria Wojskowa – lecz wyłącznie w stosunku do żołnierza pełniącego czynną służbę wojskową, wobec którego ŻW prowadzi postepowania przygotowawcze z pełnej kwalifikacji określonej treścią całego k.k.

Organy ścigania mają zapewnioną pomoc umocowaną w k.p.k. którą mogą otrzymać od osób mających wiedzę na temat przestępstw kartowych, np. skimmingu w punkcie handlowo-usługowym, gdzie na pierwszej linii reagowania na przestępczy proceder sczytywania zawartości paska magnetycznego, stoją potencjalni świadkowie, czyli np. pracodawca, lub pracownik, który zauważył fakt skanowania kart płatniczych przez kasjera. Pracodawca ponadto na podstawie art. 15 § 3 k.p.k. ma obowiązek podjęcia pełnej współpracy z organami ścigania[33], w tym przez przekazanie monitoringu, czy pełnych danych pracownika, który był sprawcą przestępstwa[34].

Policja funkcjonująca w oparciu o zapisy stosownej ustawy[35] oraz szeregu rozporządzeń ministra właściwego ds. wewnętrznych, czy zarządzeń Komendanta Głównego Policji, reagowanie na stwierdzone przestępstwa w sektorze płatności bezgotówkowych i akceptacji kart płatniczych, powierza komórkom do walki z przestępczością gospodarczą, lub komórkom dochodzeniowo-śledczym, określając je jako właściwe do prowadzenia postepowań przygotowawczych w tym zakresie, z uwagi na postrzeganie ww. rodzaju przestępczości jako przestępczość gospodarczą[36]. W każdym Wydziale dw. z PG w Komendach Wojewódzkich Policji oraz KSP, do których kompetencji należy prowadzenie czynności operacyjno-rozpoznawczych i dochodzeniowo-śledczych, w odniesieniu do przestępstw dokonywanych w obrocie bankowym i kapitałowym, związanych z obrotem gospodarczym, czy związanych z legalizacją dochodów uzyskanych z działalności przestępczej, a także fałszerstwa środków płatniczych (z wyłączeniem pieniędzy)[37], znajdują się funkcjonariusze ze specjalistycznym przeszkoleniem w zakresie zwalczania przestępstw z udziałem kart płatniczych. Posiadają oni niezbędną wiedzę oraz kontakty robocze z emitentami kart[38], a także gromadzą informacje o przestępstwach stwierdzonych przez komórki terenowe policyjnych garnizonów[39]. Ich praca jest koordynowania przez Wydział do walki z Przestępczością Gospodarczą Biura Kryminalnego KGP. Policjanci tych komórek wspierają ponadto programy profilaktyczne emitentów kart i NBP w zakresie edukacji społecznej dla wzrostu świadomości o niebezpieczeństwach, jakie czyhają na użytkowników kart[40]. W strukturach Policji znajduje się również eksperckie stanowisko krajowego koordynatora

---

33 Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego, tekst jednolity Dz.U. 2016 poz. 1749.

34 B. Kowalski, dz. cyt., s. 171.

35 Ustawa z dnia 6 kwietnia 1990 r. o Policji, tekst jednolity Dz.U. 2016 poz. 1782.

36 Informacje uzyskane z Wydziału ds. Parlamentarnych i Informacji Publicznej Gabinetu Komendanta Głównego Policji, na wniosek autora (w posiadaniu autora).

37 http://www.policja.waw.pl/pl/stoleczna-policja/wydzialy-ksp/wydzial-do-walki-z-prze/85,Wydzial-do-walki-z-Przestepczoscia-Gospodarcza.html [dostęp: 29.09.2017].

38 S. Górnicki, *Zalecenia metodyczne w zakresie gromadzenia dowodów w postępowaniach przygotowawczych w sprawach o przestępstwa kradzieży, fałszerstwa bankowych kart płatniczych oraz wprowadzania do obrotu sfałszowanych bankowych kart płatniczych*, [w:] J. Kosiński (red.), *Przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych: III Międzynarodowa Konferencja Naukowa*, Szczytno 2003, s. 106.

39 J. Biegański, Ł. Nowacki, *Zasady współpracy banków i agentów rozliczeniowych z organami ściągania*, [w:] J. Kosiński (red.), *Przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych: III Międzynarodowa Konferencja Naukowa*, Szczytno 2003, s. 111.

40 http://www.policja.pl/pol/aktualnosci/70983,Policjanci-o-skimmingu-podczas-dni-otwartych-w-NBP.html [dostęp: 29.09.2017].

ds. przestępczości kartowej, odpowiedzialnego za współpracę funkcjonariuszy zajmujących się tą problematyką z zagranicznymi kolegami, w ramach sieci krajowych ekspertów w oparciu o szyfrowane łącza wymiany informacji (Siena) pomiędzy państwami członkowskimi Europolu[41].

Z uwagi na międzynarodowy charakter przestępczości zorganizowanej związanej z wykorzystaniem kart płatniczych[42], w jej zwalczaniu bardzo istotną rolę odgrywa współpraca międzynarodowa. W ramach Europejskiego Urzędu Policji, jakim jest Europol, w jego Departamencie Operacyjnym funkcjonuje od 2003 r. zespół zadaniowy AWF Terminal (ang. *Analitycal Work File Terminal*), który powstał z inicjatywy Belgów w celu znalezienia powiązań między odrębnymi dochodzeniami oraz ułatwienia międzynarodowej wymiany informacji przy dochodzeniach dotyczących zorganizowanych siatek przestępczych zaangażowanych w proceder skimmingu[43]. Europejska wymiana informacji na temat przestępczości kartowej może polegać na wymianie raportów o powiązaniach, zawierających podstawowe informacje na temat powiązań kryminalnych pomiędzy osobami rozpracowywanymi w różnych krajach, oraz związku pomiędzy skimmingiem, a wypłatami oraz prowadzonymi w tych sprawach śledztwach przez członków Europolu. Drugą z form są raporty analityczne zawierające dogłębną analizę struktury przestępczej, obszaru działalności, oraz wyciągnięte wnioski co do kierunków dalszej współpracy międzynarodowej w konkretnej sprawie. Raporty uwzględniają dane przetwarzane w bazach danych, za jaką można uznać CardChecker, pozwalający ustalić wydawcę większości kart płatniczych emitowanych na świecie[44]. Europol w ramach AWF Terminal kładzie nacisk na wzajemne wsparcie i poza spotkaniami operacyjnymi i koordynacyjnymi organizowanymi przy prowadzaniu konkretnych spraw na płaszczyźnie międzynarodowej, a także wdrożonym systemem wczesnego ostrzegania przed zidentyfikowanym nowym modus operandi sprawców, czy nowymi technikami i urządzeniami służącymi m.in. do skimmingu, na co dzień zajmuje się wsparciem strategicznym partnerów współpracujących. Przejawia się to w szkoleniach dotyczących bezgotówkowych oszustw płatniczych, wydawaniu anglojęzycznych podręczników na ten temat, spotkaniach eksperckich i konferencjach pozwalających na wymianę doświadczeń pomiędzy koordynatorami krajowymi, czy stworzeniu mechanizmu pozwalającego na składanie sprawozdań statystycznych przestępczości kartowej z poszczególnych państw. Ponadto organizowane są spotkania z przedstawicielami organizacji płatniczych czy emitentów, gdzie funkcjonariusze zapoznają się z nowymi środkami bezpieczeństwa stosowanymi w kartach płatniczych oraz omawiają trendy współczesnej przestępczości w sektorze płatności bezgotówkowych. Europol ponadto zainicjował powstanie kolejnych grup roboczych jakimi są Centrum Informacji o Przestępczości Finansowej (ang. *Financial Crime Information Centre* – FCIC), czy zespół EAST (ang. *European ATM Security Team*), zajmujący się opracowaniem strategii działania wobec przestępczości uderzającej w ban-

41 M. Skowronek, J. Cholewiński, *Operacja kryptonim IASI*, [w:] J. Kosiński, S. Kmiotek (red.), *Przestępczość teleinformatyczna*, Szczytno 2011, s. 236.

42 W. Mądrzejowski, *Przestępczość zorganizowana. System zwalczania*, Warszawa 2015, s. 89.

43 Europol, *Bezgotówkowe oszustwa płatnicze*, [w:] J. Kosiński (red.), *Przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych. Materiały konferencyjne*, Szczytno 2006, s. 155.

44 M. Skowronek, J. Cholewiński, dz. cyt., s. 237.

komaty. W ramach ATM Terminal. Europol ponadto wspiera kwestię analizy technicznej sfałszowanych kart płatniczych w oparciu o UCS – Uniwersalny System Klasyfikacji Sfałszowanych Kart Płatniczych (ang. *Universal Calssification System fot Counterfeit Payment Cards*), za sprawą którego istnie możliwość rozpoznawania i szukania powiązań pomiędzy przestępstwami kartowymi z różnych państw europejskich dzięki bazą wyników technicznego badania kart, ich fotografii i informacji technicznych nt. sfałszowanych kart[45].

W Polsce kryminalistyczne badania kart płatniczych przeprowadza Zakład Badań Dokumentów i Technik Audiowizualnych Centralnego Laboratorium Kryminalistycznego Policji, lub zespoły bądź sekcje właściwe do badań dokumentów z Laboratoriów Kryminalistycznych Komend Wojewódzkich (lub Stołecznej) Policji. Dodatkowo CLKP stara się poszerzyć zakres przetwarzanych katalogów danych, o bazę elektronicznych środków płatniczych[46]. W kwestii ustaleń teleinformatycznych w związku z przestępstwami kartowymi, z uwagi na przeznaczenie właściwe są komórki do walki z cyberprzestępczością, koordynowane przez Biuro do Walki z Cyberprzestępczością KGP. Wspominane piony co istotne – nie prowadzą pracy procesowej[47].

Kwestię działań podejmowanych przez funkcjonariuszy Policji w odniesieniu do zidentyfikowanej przestępczości w sektorze płatności bezgotówkowych i akceptacji kart płatniczych, regulują m.in. zarządzenie pf-634 Komendanta Głównego Policji z dnia 30 czerwca 2006 r. w sprawie metod i form wykonywania przez Policję czynności operacyjno-rozpoznawczych[48] (z późn. zm.), a także decyzja nr 252 Komendanta Głównego Policji z dnia 18 kwietnia 2008 r. w sprawie programu kursu specjalistycznego w zakresie zwalczania przestępczości gospodarczej (z późn. zm.)[49][50].

W kwestii ustalenia informacji o dowodach przy stwierdzeniu przestępczości kartowej, S. Górnicki wskazuje na typologię źródeł w oparciu o poszczególne podmioty funkcjonujące na rynku transakcji bezgotówkowych:

- akceptant płatności (punkt handlowo-usługowy):
  przesłuchanie pracowników (kasjerów) obsługujących podejrzaną transakcję, lub stwierdzony fraud pozwala na:
  a. ustalenie rysopisu domniemanego sprawcy,
  b. zabezpieczenie oryginału dokumentu potwierdzającego dokonanie płatności bezgotówkowej,
  c. zabezpieczenie nagrań monitoringu akceptanta, lub z obiektu gdzie znajduje się punkt handlowo-usługowy akceptanta;
- bank – emitent i właściciel karty:
  współpraca z emitentem karty płatniczej pozwala organom ścigania na:

45 Europol, dz. cyt., s. 156–160.

46 http://clk.policja.pl/clk/clkp/historia/historia/66039,Historia-laboratorium.html [dostęp: 29.09.2017].

47 Informacje uzyskane z Wydziału ds. Parlamentarnych i Informacji Publicznej Gabinetu Komendanta Głównego Policji, na wniosek autora (w posiadaniu autora).

48 Dokument niepublikowany.

49 Dz. Urz. KGP poz. 58, z 2013 r. poz. 13, oraz z 2015, poz. 21.

50 Informacje uzyskane z Wydziału ds. Parlamentarnych i Informacji Publicznej Gabinetu Komendanta Głównego Policji, na wniosek autora (w posiadaniu autora).

a. uzyskanie wszystkich informacji na temat kwestionowanych transakcji dokonanych przy użyciu skradzionej lub sfałszowanej karty,
b. wskazanie agenta rozliczającego daną transakcję,
c. wskazanie faktycznego posiadacza karty;

- acquirer – agent rozliczeniowy, centrum operacyjno-rozliczeniowe acquirera:
  Współpraca organów ścigania z agentem rozliczeniowym polega na:
  a. ustalenie adresu akceptanta kwestionowanych transakcji;
  b. ustalenie miejsca gromadzenia dokumentacji z przeprowadzonych transakcji;
  c. uzyskanie opinii i informacji na temat prawidłowości przeprowadzenia transakcji u danego akceptanta:
     I. czy pojawiały się fraudy?
     II. czy występowały rażące naruszenia procedury akceptacji kart płatniczych, bądź inne okoliczności mogące podważać zaufanie do prawidłowości obsługiwania terminala POS przez personel placówki?
- organizacja płatnicza również może udzielić informacji organom ścigania, jeśli informacje z powyższych źródeł nie pozwalają na pełne wyjaśnienie okoliczności zdarzenia, aczkolwiek podmiotem dedykowanym do udzielania niezbędnych informacji na temat karty płatniczej dla potrzeb postepowania karnego, jest emitent karty (bank wydawca lub organizacja płatnicza), którego dane są nadrukowane na jej rewersie[51].

Podsumowanie

Specyfikacja zagrożeń związanych z obrotem bezgotówkowym skupia się wokół naruszenia tajności danych, nieautoryzowanego dostępu do systemu, czy zablokowania pewnych usług bankowych[52]. Za zagrożenie można również uznać samą szybkość wymiany i dostępność informacji dotyczących sposobów popełniania przestępstw, a także wykorzystywanie luk organizacyjnych, technologicznych czy prawnych[53]. Powszechność obrotu bezgotówkowego w wielu formach, przekłada się ponadto na szeroki wachlarz zdefiniowanych działań przestępczych, m.in.: kradzieży karty płatniczej, fałszerstwa karty płatniczej, posługiwania się kartami płatniczymi niedoręczonymi do prawnego posiadacza, wyłudzenia karty w oparciu o wniosek z nieprawdziwymi danymi, *skimmingu* karty bankomatowej, *cardingu* – czyli dysponowania cudzymi środkami płatniczymi z wykorzystaniem danych cudzej karty płatniczej, *phishingu* i *vishingu* – czyli kradzieży tożsamości, *pharmingu* – czyli przekierowania do fałszywej strony internetowej, *sniffingu* – czyli podsłuchu w Internecie, *tamperingu* – czyli penetracji w celu przechwycenia danych oraz *spoofingu* – czyli podszywania się pod inną tożsamość.

Problematyka bezpieczeństwa transakcji dokonywanych kartami płatniczymi jest zdaniem R. Kaszubskiego wypadkową działań podejmowanych zarówno przez wydawców, agentów rozliczeniowych, akceptantów i posiadaczy kart. Nie sposób nie zgodzić się

[51] S. Górnicki, dz. cyt., s. 104–105.
[52] W. Chmielarz, *Systemy elektronicznej bankowości i cyfrowej płatności*, Warszawa 1999, s. 105.
[53] D. Cyman, dz. cyt., s. 237.

z kolejnym twierdzeniem wspomnianego autora, iż tylko w przypadku właściwego funkcjonowania tych wszystkich elementów składowych systemu, możliwe będzie utrzymanie w Polsce dotychczasowego, ocenianego jako bardzo wysoki, w porównaniu do innych krajów, poziomu bezpieczeństwa rynku kart płatniczych[54].

Tytuł w języku angielskim:
MODERN CRIMINALITY ASSOCIATED WITH ELECTRONIC MONEY: THE ROLE OF POLICE INVESTIGATOR

Bibliografia

Dokumenty i materiały źródłowe

Ustawa z dnia 6 kwietnia 1990 r. o Policji, tekst jednolity Dz.U. 2016 poz. 1782.

Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego, tekst jednolity Dz.U. 2016 poz. 1749.

Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych, tekst jednolity Dz.U. 2016 poz. 1572.

Dyrektywa 2000/46/EC Parlamentu Europejskiego i Rady z dnia 18 września 2000 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalności, Dz. U. L 275/39 z 21 października 2000 r.

Dyrektywa 2009/110/WE Parlamentu Europejskiego i Rady z dnia 16 września 2009 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością, zmieniająca dyrektywy 2005/60/WE i 2006/48/WE oraz uchylająca dyrektywę 2000/46/WE, Dz. U. L 267/7 z 10 października 2009 r.

Dz. Urz. KGP poz. 58, z 2013 r. poz. 13, oraz z 2015. poz. 21.

Informacje uzyskane z Wydziału ds. Parlamentarnych i Informacji Publicznej Gabinetu Komendanta Głównego Policji, na wniosek autora (w posiadaniu autora).

Książki i artykuły

Biegański J., Nowacki Ł., *Zasady współpracy banków i agentów rozliczeniowych z organami ściągania*, [w:] *Przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych: III Międzynarodowa Konferencja Naukowa*, Kosiński J. (red.), Szczytno 2003.

Chmielarz W., *Systemy elektronicznej bankowości i cyfrowej płatności*, Warszawa 1999.

Cyman D., *Elektroniczne instrumenty płatnicze a bezpieczeństwo użytkowników rynku finansowego*, Warszawa 2013.

Europol, *Bezgotówkowe oszustwa płatnicze*, [w:] *Przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych. Materiały konferencyjne*, Kosiński J. (red.), Szczytno 2006.

Flajterski S., Świecka B., *Elementy finansów i bankowości*, Warszawa 2007.

Gąsiorowski J., Podsiedlik P., *Przestępstwa w bankowości elektronicznej w Polsce. Próba oceny z perspektywy prawno-kryminalistycznej*, Dąbrowa Górnicza 2015.

Górnicki S., *Zalecenia metodyczne w zakresie gromadzenia dowodów w postępowaniach przygotowawczych w sprawach o przestępstwa kradzieży, fałszerstwa bankowych kart płatniczych oraz wprowadzania do*

[54] *Bezpieczeństwo prawne transakcji dokonywanych kartami płatniczymi*, „Gazeta Prawna" z dn. 11.12.2008 r.

obrotu sfałszowanych bankowych kart płatniczych, [w:] *Przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych: III Międzynarodowa Konferencja Naukowa*, J. Kosiński (red.), Szczytno 2003.

Grzybowska A., *Innowacyjne rozwiązania na rynku usług płatniczych*, [w:] *Stan i perspektywy rozwoju współczesnej bankowości*, Mikulska T., Sikorski J. (red.), Białystok 2014.

Janowicz R., *Pieniądz elektroniczny na świecie*, [w:] *Przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych*, Kosiński J. (red.), Szczytno 2003.

Kosiński J., *Paradygmaty cyberprzestępczości*, Warszawa 2015.

Kowalski B., *Problematyka przestępstw dotyczących kart płatniczych na przykładzie skimmingu i cardingu*, „Przegląd Policyjny" 2015, Nr 4(120).

Laskowska K., *Działalność zorganizowanych grup przestępczych z udziałem cudzoziemców w Polsce w latach 2004–2013 w świetle policyjnych badań statystycznych*, „Przegląd Policyjny" 2016, nr 3(123).

Mądrzejowski W., *Przestępczość zorganizowana. System zwalczania*, Warszawa 2015.

Michór A., *Karty płatnicze*, [w:] *Problemy współczesnej bankowości. Zagadnienia prawne*, Góralczyk W. (red.), Warszawa 2014.

Mikołajczyk K., *Przestępstwa związane z wykorzystywaniem bankowości elektronicznej – skimming*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 10(6).

Mikos-Sitek A., Zapadka P., *Polskie prawo bankowe. Wybrane zagadnienia*, Warszawa 2011.

Olszar P., *Złośliwe oprogramowanie w bankowości elektronicznej*, [w:] *Przestępczość teleinformatyczna*, Kosiński J. (red.), Szczytno 2013.

Pacak M., *Ustawa o elektronicznych instrumentach płatniczych. Komentarz*, Warszawa 2013.

Prokopiuk A., *Wybrane aspekty rozwoju e-bankowości w Polsce*, [w:] *Stan i perspektywy rozwoju współczesnej bankowości*, Mikulska T., Sikorski J. (red.), Białystok 2014.

Skowronek M., Cholewiński J., *Operacja kryptonim IASI*, [w:] *Przestępczość teleinformatyczna*, Kosiński J., Kmiotek S. (red.), Szczytno 2011.

Wilczewski R., *Phishing – popełnianie i zwalczanie*, [w:] *Przestępczość teleinformatyczna*, Kosiński J., Kmiotek S. (red.), Szczytno 2011.

Prasa i inne

Bezpieczeństwo prawne transakcji dokonywanych kartami płatniczymi, „Gazeta Prawna" z dn. 11.12.2008 r.

Kradzież w Polsce, wypłata w Peru, „Rzeczpospolita" z dn. 12.01.2015 r.

Nie zawsze warto kartą, „Dziennik Trybuna" z dn. 11.02.2015 r.

Źródła internetowe

http://clk.policja.pl/

http://www.policja.waw.pl/

http://www.policja.pl/