Mateusz Staszczyk

Nieuprawnione transakcje bankowe jako przejaw cyberprzestępczości

Finanse i Prawo Finansowe 2/1, 43-56

2015

Artykuł został opracowany do udostępnienia w internecie przez Muzeum Historii Polski w ramach prac podejmowanych na rzecz zapewnienia otwartego, powszechnego i trwałego dostępu do polskiego dorobku naukowego i kulturalnego. Artykuł jest umieszczony w kolekcji cyfrowej bazhum.muzhp.pl, gromadzącej zawartość polskich czasopism humanistycznych i społecznych.

Tekst jest udostępniony do wykorzystania w ramach dozwolonego użytku.

MUZEUM HISTORII POLSKI

• F I N A N S E I P R A W O F I N A N S O W E •
• Journal of Finance and Financial Law •

Marzec/March 2015 • vol. II, no. 1 ISSN 2353-5601

NIEUPRAWNIONE TRANSAKCJE BANKOWE JAKO PRZEJAW CYBERPRZESTĘPCZOŚCI

Mateusz Staszczyk*

Streszczenie:

Opracowanie ma na celu wskazanie na jedno z kluczowych wyzwań, jakim jest funkcjonowanie sektora bankowego wobec rosnących przypadków fraudów bankowych. W artykule zanalizowano tą tematykę poprzez kilka podpunktów. W pierwszej kolejności zdefiniowano pojęcie fraudów, a także przedstawiono powiązaną z tym cyberprzestępczość. Następnie przytoczono kilka przykładów ataków na systemy bankowe i opisano ślady elektroniczne, które pozostawiają te ataki. Na zakończenie wskazano sposoby walki ze zjawiskiem fraudów bankowych.

Słowa kluczowe: fraudy, bankowość elektroniczna, cyberprzestępczość.

JEL Class: G21, L86.

Przyjęto/Accepted : 10.03.2015 Opublikowano/Published: 30.03.2015

WPROWADZENIE

Według danych przekazywanych przez banki, w II półroczu 2013 r. liczba operacji oszukańczych dokonanych kartami płatniczymi wyniosła 29,6 tys., natomiast według danych otrzymanych od agentów rozliczeniowych liczba ta osiągnęła poziom 11,6 tys. Sektor finansowy jest celem wyrafinowanych działań przestępczych, głównie z powodu wartości aktywów, jakimi się tam zarządza.

* Mgr, doktorant, Instytut Finansów, Wydział Ekonomiczno-Socjologiczny, Uniwersytet Łódzki.

Marzec/March 2015 • vol. II, no. 1 ISSN 2353-5601

Wyścig o pierwszeństwo w wygodnej sprzedaży – on-line – staje się dla przestępców okazją do wyłudzeń. To powoduje, że banki i inne instytucje finansowe mają przed sobą do zarządzania konflikt między wygodną dla klientów sprzedażą a utrzymaniem jej bezpieczeństwa tak, aby „wygoda" nie stawała się okazją dla przestępców. Stąd ważne jest, aby skuteczność zarządzania tym konfliktem była dostrzegana przez regulatora rynku [*III Kongres antyfraudowy – podsumowanie z debaty kongresowej*..., 2012: 10].

Problematykę zagrożeń systemu bankowego należy rozpocząć od kilku tez, a mianowicie [Jaroch 2013: 57]:

– przestępczość przeciwbankowa stanowi i będzie stanowić istotny oraz stały element przestępczości związanej z obrotem gospodarczym,

– w kategorii przestępstw przeciwbankowych pojawiają się szczególnego rodzaju czyny przestępcze polegające na przestępczym wykorzystaniu technologii komputerowych.

Celem niniejszego artykułu jest wskazanie na jedno z kluczowych wyzwań, jakim jest funkcjonowanie banków wobec rosnących przypadków fraudów bankowych. Dokonano tego poprzez analizę kilku podpunktów m. in.: cyberprzestępczość i ślady elektroniczne.

1. CO TO SĄ FRAUDY BANKOWE

Fraud (transakcja nieuprawniona) – transakcja kartą płatniczą zakwestionowana przez bank, wystawcę karty. Za transakcje fraud uważa się transakcje (lub próby transakcji) kartami skradzionymi, zagubionymi (zastrzeżonymi), skopiowanymi lub otrzymanymi na podstawie fałszywych danych lub danych obcego właściciela. Transakcje fraud to coraz częściej oszustwa przy użyciu kart skopiowanych na zasadzie *skimmingu* w bankomatach lub samoobsługowych automatach akceptujących karty (np. na stacji benzynowej). W przypadku transakcji fraud, sprzedawca (akceptant) po zobaczeniu odpowiedniego komunikatu na wyświetlaczu terminala płatniczego, powinien zatrzymać kartę [http://finansopedia.forsal.pl/wiki/Fraud].

Średnio 0,9% – tyle każdego roku przychodu generowanego przez sklep internetowy jest pochłaniane przez fraudy, czyli transakcje, które zostały wygenerowane przez skradzione lub fałszywe karty kredytowe. Tak wynika z raportu firmy CyberSource Corp. Zgodnie z amerykańskim prawem, bo o tym regionie mowa, w takich przypadkach stratę ponosi sklep sprzedający towar. Raport dodaje, że urządzenia mobilne są coraz częściej przedmiotem tych samych zagrożeń, co komputery. W tym złośliwego oprogramowania, które może wejść do

Marzec/March 2015 • vol. II, no. 1 ISSN 2353-5601

urządzenia za pośrednictwem poczty e-mail lub w inny sposób i kradzieży danych karty kredytowej, konta i innych poufnych informacji[1].

W związku z tymi liczbami aż 1/3 właścicieli sklepów internetowych w Stanach deklaruje iż zwiększą budżety związane z zarządzaniem ryzykiem wynikającym z transakcji fraudowych. Łączna wartość tego typu kradzieży wyniosła w 2012 r. 3,5 miliarda dolarów. Czytając te dane właściciele polskich sklepów internetowych mogą odetchnąć ze spokojem, że prowadzą interes w kraju w którym rozpowszechnienie kart kredytowych jest dużo mniejsze a winę za dopuszczenie do transakcji fraudowej zwykle ponosi *provider* serwisu płatności elektronicznych[2].

Fraudy powiązane są z ryzykiem operacyjnym polegającym między innymi na trudnościach z jego precyzyjnym opisaniem. Definicja Bazylejskiego Komitetu Nadzoru Bankowego w praktyce nie wystarcza do zarządzania ryzykiem. Instytucje zarządzające ryzykiem muszą wypracować ściślejsze metody określania, gdzie występuje ryzyko operacyjne. Z tego względu Komitet Bazylejski, a za jego przykładem również inne instytucje nadzorcze, między innymi Komisja Nadzoru Bankowego, wyróżniły 7 ogólnych kategorii strat operacyjnych. Są one następujące [Piołunowicz 2006: 52]:

– oszustwo wewnętrzne (*internal fraud*),
– oszustwo zewnętrzne (*external fraud*),
– praktyka kadrowa i bezpieczeństwo pracy (*employment practices and workplace safety*),
– klienci, produkty i praktyka biznesowa (*clients, products and business practices*),
– uszkodzenia aktywów (*damage to physical assets*),
– zakłócenia działalności i błędy systemów (*business disruptions and system failures*),
– dokonywanie transakcji, dostawa oraz zarządzanie procesami (*execution, delivery and process management*).

2. CYBERPRZESTĘPCZOŚĆ

Na całym świecie cyberprzestępczość jest wielkim problemem, którego znaczenie wciąż wzrasta. W obliczu globalizacji, ochrona cyberprzestrzeni stała się jednym z podstawowych celów strategicznych w obszarze bezpieczeństwa każdego państwa. W czasie, gdy panuje swoboda przepływu osób, towarów, informacji i kapitału – bezpieczeństwo demokratycznego państwa zależy od

[1] Prawie 1% rocznych przychodów sklepów internetowych pochłaniają fraudy!, w: http://www. handelinternetowy.pl/prawie-1-rocznych-przychodow-sklepow-internetowych-pochlaniaja-fraudy/, dostęp: 17.09.2013.

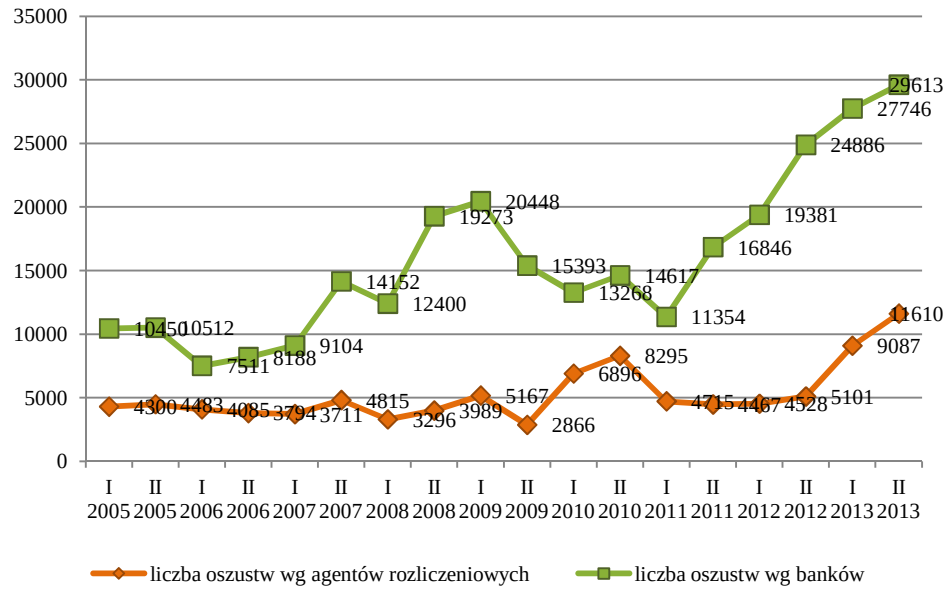
[2] http://www.handelinternetowy.pl/prawie-1-rocznych-przychodow-sklepow-internetowych-pochlaniaja-fraudy/, dostęp: 17.09.2013.

Marzec/March 2015 • vol. II, no. 1 ISSN 2353-5601

wypracowania mechanizmów pozwalających skutecznie zapobiegać i zwalczać zagrożenia dla bezpieczeństwa cyberprzestrzeni [*Rządowy Program Ochrony Cyberprzestrzeni na lata 2011–2016*...].

Ogólnie grupa czynów, określana jako cyberprzestępstwa, polega na posługiwaniu się sieciami telekomunikacyjnymi do naruszania jakiegokolwiek dobra prawnego chronionego przez prawo karne. Za najistotniejsze cechy cyberprzestępczości można uznać działanie w specyficznym środowisku genetycznie związanym z technologią komputerową i wykorzystywanie go do popełniania przestępstw pospolitych (np. oszustwo, fałszerstwo dokumentu), jak i mniej konwencjonalnych (np. *cracking*, *hacking*, *phising*) [Siwicki 2013: 19–20].

Narodowy Bank Polski przygotował ocenę funkcjonowania systemu płatniczego w okresie lipiec–grudzień 2013 r. NBP zwraca uwagę, że w drugiej połowie ubiegłego roku w porównaniu z pierwszą aż o 6,7 proc. wzrosła liczba oszustw kartowych (wykres 1), przez specjalistów określanych mianem fraudów. Statystyki za okres od lipca do grudnia są najgorsze co najmniej od 2005 r., czyli od czasu, kiedy NBP publikuje informacje na ten temat [Uryniuk, *Złodzieje*..., dostęp: 24.04.2014].



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

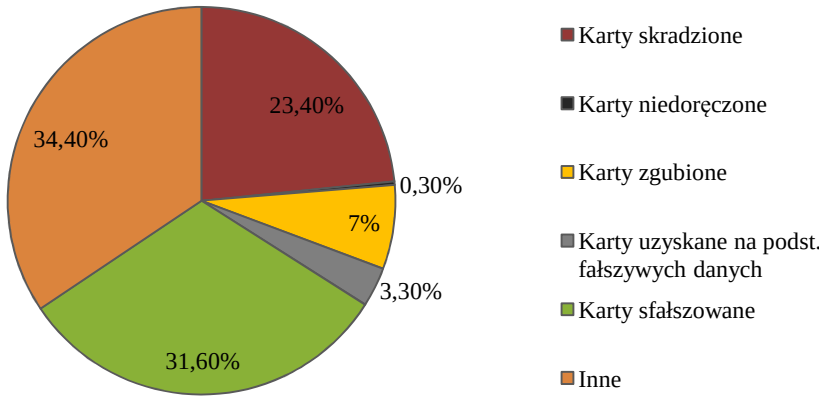
Źródło: NBP [2014: 68].

Marzec/March 2015 • vol. II, no. 1 ISSN 2353-5601

Za wzrost liczby transakcji oszukańczych kartami odpowiada też coraz większa aktywność cyberprzestępców. Za pomocą różnych zabiegów socjotechnicznych w sieci pozyskują oni informacje o kartach użytkowników. Dane te są następnie wykorzystywane do kradzieży w Internecie czy też w terminalach stacjonarnych [Uryniuk, *Złodzieje*..., dostęp: 24.04.2014].

Za wzrost fraudów może też odpowiadać upowszechnienie się kart bezstykowych, które pozwalają na dokonywanie transakcji bez autoryzacji kodem PIN. Przemawia za tym spadająca średnia wartość pojedynczego oszustwa. Ze względu na to, że bez autoryzacji PIN-em możliwe są jedynie transakcje do 50 zł, nie powinno to wpływać znacząco na wzrost wartości wszystkich fraudów [Uryniuk, *Złodzieje*..., dostęp: 24.04.2014].

Według danych NBP w II poł. ubiegłego roku najwięcej fraudów odnotowano w kategorii „inne" (wykres 2), gdzie banki wykazują m. in. oszustwa internetowe. Ich udział we wszystkich kradzieżach wyniósł 34,4 proc., choć w porównaniu z poprzednim raportem zmniejszył się o 8,6 pkt proc. Na drugim miejscu pod względem popularności są fraudy kartami sfałszowanymi, których było 31,6 proc., co oznacza wzrost w porównaniu z I poł. 2013 r. o 2,7 pkt proc. Do 23,4 proc. wzrósł również udział transakcji oszukańczych kartami skradzionymi. W poprzednim raporcie było ich 19 proc. Bank centralny podaje, że rośnie również liczba kradzieży kartami zgubionymi, które stanowiły 7 proc. wszystkich oszustw [Uryniuk, *Złodzieje*..., dostęp: 24.04.2014].

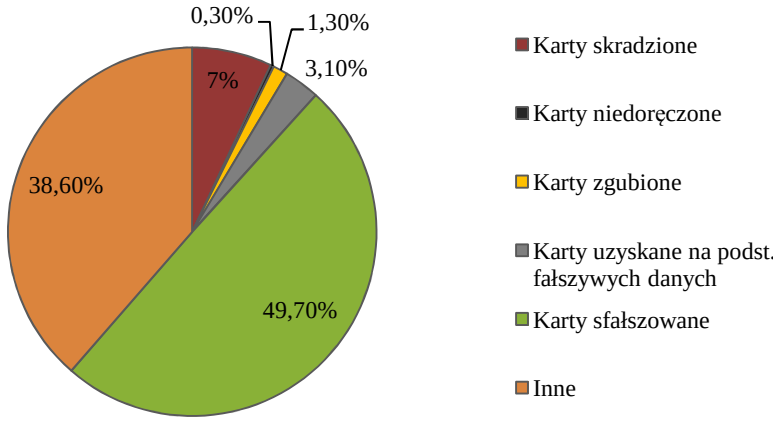


Wykres 2. Struktura operacji oszukańczych kartami płatniczymi według liczby w II półroczu 2013 r.

Źródło: NBP [2014: 69].

Marzec/March 2015 • vol. II, no. 1 ISSN 2353-5601

Pod względem wartości 49,7 proc. stanowiły operacje oszukańcze dokonane za pomocą kart sfałszowanych, 38,6 proc. „innych", a 7 proc. kart skradzionych (wykres 3).



Wykres 3. Struktura operacji oszukańczych kartami płatniczymi według wartości w II półroczu 2013 r.

Źródło: NBP [2014: 71].

Bankowcy podkreślają, że mimo wzrostu liczby kartowych transakcji oszukańczych Polska wciąż jest krajem o jednym z najniższych w Europie współczynniku tego typu przestępstw. Narodowy Bank Polski podkreśla, że oszukańcze operacje kartowe stanowią zaledwie 0,02 proc. wartości wszystkich transakcji dokonanych kartami płatniczymi. Nawet Europejski Bank Centralny podkreśla, że jesteśmy pod tym względem prymusem w całej Europie [Uryniuk, *Złodzieje...*, dostęp: 24.04.2014]. Co więcej, dane statystyczne nie przekładają się na straty ponoszone przez klientów. W procesie reklamacyjnym najczęściej otrzymują oni zwrot środków.

Zastąpienie paska mikroprocesorem to technologiczny przełom. Dzięki pojemności czipa do potwierdzenia każdej transakcji używa się tzw. dynamicznej autentykacji autoryzacji (DDA), co oznacza, że przy każdej płatności w sklepie czy też wypłacie pieniędzy w bankomacie mikroprocesor karty kontaktuje się z centrum autoryzacyjnym, szyfrując połączenie przy pomocy innego klucza. Skopiowanie danych zawartych w mikroprocesorze karty spowoduje, że komputer w centrum autoryzacyjnym wykryje przestępstwo i nie potwierdzi transakcji [Uryniuk 2011: G1].

Postęp technologiczny następuje także w autoryzacji transakcji internetowych. Dziś nie wystarczy już podanie numeru karty i daty jej ważności, by kartą zapłacić w sklepie internetowym. Wymagany jest tzw. *securcode*. Można go

Marzec/March 2015 • vol. II, no. 1 ISSN 2353-5601

uzyskać za pomocą SMS-a lub tokena. Najnowsze rozwiązania zmierzają do tego, by hasła SMS-owe lub z tokena zastąpić hasłami generowanymi przez same karty. Dlatego są one wyposażane w klawiaturę dotykową, dzięki której możemy wystukać PIN, oraz w wyświetlacz LCD, na którym widoczne jest generowane przez mikroprocesor karty hasło jednorazowe, służące do potwierdzenia transakcji w sieci [Uryniuk 2011].

W lipcu 2013 r. Europejski Bank Centralny opublikował po raz drugi materiał pt. *Report on card fraud*, w którym zaprezentował analizę danych statystycznych dotyczących oszustw z użyciem kart płatniczych w krajach UE w 2011 r. Dane zostały przekazane do EBC przez prawie wszystkie funkcjonujące w Europie systemy kart płatniczych, zarówno międzynarodowe (VISA, MasterCard), jak i systemy lokalne [NBP 2013: 30].

Dane wskazują, że w Polsce odnotowano jeden z najmniejszych udziałów transakcji oszukańczych w wartości wszystkich transakcji dokonanych kartami. Stawia to Polskę pod względem bezpieczeństwa na bardzo wysokim, drugim miejscu, za Rumunią, która w 2011 r. wyprzedziła Polskę, będącą liderem w 2010 r. Z danych raportu wynika także, że udział liczby transakcji oszukańczych w ogólnej liczbie wszystkich transakcji dokonanych w Polsce w 2011 r. był najniższy spośród wszystkich krajów UE i wyniósł 0,001%. W przypadku niektórych krajów występuje duża rozbieżność pod względem danych przekazywanych przez agentów rozliczeniowych jak i wydawców kart płatniczych [NBP 2013: 30–31].

Ważnym aspektem wpływającym na tak niski poziom oszustw dokonywanych kartami płatniczymi są działania podejmowane przez sektor bankowy we współpracy z Policją i Prokuraturą [NBP 2013: 31].

Według raportu z 2013 r. o cyberprzestępczości przygotowanego przez Symatec [Góra 2014]:

– koszt przypadający na ofiarę cyberprzestępczości wzrósł o 50%,

– 6 milionów Polaków padło ofiarą cyberprzestępców,

– koszty związane z działalnością przestępców internetowych wyniosły w Polsce 6 miliardów złotych,

– tylko 28% używa podstawowych programów zabezpieczających na smartfonach,

– 50% użytkowników smartfonów nie kasuje maili od nieznanych nadawców,

– 21% polskich rodziców pozwala dzieciom korzystać ze swoich służbowych urządzeń,

– 31% Polaków dzieli się z innymi swoimi hasłami do mediów społecznościowych.

Wskazuje się, że cechą charakterystyczną przestępczości *stricte* komputerowej jest niewielka gotowość ofiar przestępstw do angażowania policji w ich ściganie, pomimo relatywnie wysokich szkód, jakie czyny te w ocenie pokrzyw-

Marzec/March 2015 • vol. II, no. 1 ISSN 2353-5601

dzonych powodują. Przestępczość komputerową charakteryzują ponadto: duża „ciemna liczba", niskie prawdopodobieństwo wykrycia sprawcy oraz lekceważenie przez pokrzywdzonych środków bezpieczeństwa [Adamski 2000: 17–24].

3. STUDIUM PRZYPADKU

Jednym z przykładów złośliwego oprogramowania jest „Zeus/Citadel", który atakuje komputery użytkowników systemu Windows, a po zainstalowaniu podsłuchuje wszystkie przesyłane informacje (w tym głównie loginy i hasła) oraz – jeżeli posiada dodatkowe instrukcje w pliku konfiguracyjnym – dokonuje podmiany treści wybranych stron internetowych tuż przed ich wyświetleniem. Ponieważ zainfekowanie komputera umożliwia modyfikację treści strony banku, atakujący może wyświetlić na monitorze dowolny komunikat. Sposób ataku i treść komunikatów ograniczone są jedynie przez inwencję twórczą przestępców (którzy cały czas mają pełną kontrolę nad komputerem). Jest to przykład połączenia metod socjotechniki oraz przejęcia kontroli nad komputerem ofiary. Użytkownik będzie przeświadczony, iż czytane przez niego komunikaty pochodzą od banku – pojawiły się przecież po zalogowaniu na konto i ponadto są podpisane „dział bezpieczeństwa Twojego Banku". Poniżej przedstawiono zestawienie możliwych skutków zmian dokonywanych przez złośliwe oprogramowanie [Liszkiewicz 2014]:

– podmiana numeru konta docelowego oraz kwoty tuż przed zatwierdzeniem przelewu,
– podmiana aktualnego stanu konta,
– modyfikacja danych na liście wykonywanych operacji,
– okno proszące o podanie kodów jednorazowych w celu aktywacji/sprawdzenia funkcji bezpieczeństwa,
– okno proszące o podanie numeru telefonu oraz wybraniu modelu aparatu (atak ZitMo/2011),
– monit proszący o zwrot środków pochodzących z błędnego/podejrzanego przelewu,
– monit proszący o wykonanie testowego przelewu w ramach aktywacji/sprawdzenia nowych funkcji bezpieczeństwa.

Złośliwe oprogramowanie posiada możliwość podmieniania treści stron wyświetlanych na zainfekowanym komputerze. Nie ma znaczenia czy połączenie było szyfrowane, ponieważ wprowadzenie zmian odbywa się na komputerze ofiary, po odszyfrowaniu danych. Użytkownik nie ma żadnej możliwości weryfikacji, czy strona którą ogląda nie została zmodyfikowana przed wyświetleniem. Wprowadzane zmiany mogą być różne: od prostej zmiany jednego słowa – aż po doklejenie potężnych skryptów zawierających wiele linii kodu [Liszkiewicz 2014].

Marzec/March 2015 • vol. II, no. 1 ISSN 2353-5601

Omawianymi trojanami można się zarazić nie tylko poprzez odwiedzanie budzących wątpliwość stron internetowych, ale także przez otwarcie złośliwego załącznika przesłanego w mailu. Ponadto coraz częściej obserwowane są infekcje następujące po odwiedzeniu stron, które padły wcześniej ofiarą cyberprzestępców. W przypadku źle zabezpieczonych serwisów cyberprzestępcy mogą zaatakować je umieszczając na nich złośliwy kod, który wykonuje się w chwili otwarcia strony. Już po chwili system jest zainfekowany najnowszymi odmianami trojana ZeuS, które do chwili odwiedzenia strony bankowości elektronicznej pozostają w hibernacji [Liszkiewicz ROK]. ZeuS-p2p oraz Citadel pozostają nieaktywne do momentu zalogowania się przez ofiarę w systemie transakcyjnym swojego banku. Oba trojany działają podobnie i tuż po zalogowaniu sprawdzają saldo danego konta oraz podmieniają zawartość strony serwisu banku.

4. ŚLADY ELEKTRONICZNE I INFORMATYKA ŚLEDCZA

Banki walcząc z cyberprzestępcami wykorzystują informatykę śledczą, badając ślady elektroniczne. Ślad elektroniczny to [Witański 2014]:

– każda informacja zapisana w postaci binarnej,
– efekt działania każdego urządzenia elektronicznego,
– informacja o czynnościach (operacjach) wykonanych przez urządzenie elektroniczne.

Ślady elektroniczne w instytucji – zawartość baz danych (rachunki i kredyty), logi urządzeń elektronicznych znajdujących się w sieci informatycznej instytucji. Ślady elektroniczne poza instytucją – internet (portale informacyjne, media społecznościowe), media tradycyjne (prasa, w tym branżowa oraz kanały informacyjne tv) [Liszkiewicz 2014].

Informatyka śledcza (*Computer Forensics*) to proces poszukiwania i analizy danych zapisanych na różnego rodzaju nośnikach cyfrowych. Specjaliści informatyki śledczej składają w jedną całość strzępki informacji ukryte w gąszczu zer i jedynek, zapisanych na komputerowych dyskach. Celem jest złożenie tych fragmentów w elektroniczny odcisk palca oraz jego zabezpieczenie w taki sposób, by mógł pełnić rolę dowodu [Góra 2014].

Tradycyjna informatyka śledcza to [Góra 2014]:

– analiza *post mortem*,
– bloker i praca na kopii dysku,
– statyczny system,
– odszukiwanie i odzyskiwanie danych,
– pełna rozliczalność.

Informatyka śledcza – *live forensic* to natomiast [Góra 2014]:

– praca „na żywym organizmie”,
– dynamiczny system,

Marzec/March 2015 • vol. II, no. 1 ISSN 2353-5601

– bezpośrednio lub zdalnie,
– dostęp do aktywnych procesów,
– dostęp do zaszyfrowanych zasobów.

Informatyka śledcza w zależności od potrzeb może spełniać dwie funkcje [Liszkiewicz 2014]:

– informacyjną – na etapie prowadzenia dochodzenia dostarcza wskazówek i śladów, które umożliwiają dalsze zgłębianie interesujących zagadnień,

– dowodową – na etapie procesowym umożliwia niepodważalne udowodnienie popełnienia określonych czynów lub posiadania określonych informacji w postaci dowodu cyfrowego.

5. REKOMENDACJE DLA BANKÓW

Współpraca operacyjna pomiędzy bankami, na wypadek zajścia cyberataków dotyczących całego sektora, wymaga zacieśnienia. Niezbędne jest uregulowanie zasad współpracy pomiędzy zaatakowanymi bankami, mimo konkurowania ze sobą w świadczeniu usług bankowych. Regulacja powinna obejmować w szczególności [Bojanowski 2013]:

– zasady wymiany danych operacyjnych, w tym warunki, sposoby oraz zakres dzielenia się informacją oraz ochronę tej informacji,

– zasady udzielania wsparcia w odpieraniu ataku, w tym warunki jego udzielenia, role i odpowiedzialność współpracujących.

Banki powinny realizować zalecenia w przedmiotowym zakresie wynikające z Rekomendacji D KNF dotyczącej zarządzania obszarem technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach – rek. 18.9 – Zaleca się nawiązanie stałej współpracy z innymi bankami w zakresie wymiany informacji o zidentyfikowanych zagrożeniach oraz wniosków i doświadczeń wynikających z analizy zidentyfikowanych przypadków naruszeń bezpieczeństwa środowiska teleinformatycznego. Sposób oraz zakres wymienianych informacji powinny zapewniać ich poufność, w szczególności dochowanie tajemnicy bankowej [Bojanowski 2013].

Należy określić zakres koniecznej i rekomendowanej informacji, która powinna być przekazywana przez banki do innych podmiotów sektora bankowego, a w szczególności do podmiotu nadzorującego rynek finansowy jakim jest KNF. Budowę mechanizmów obrony i rozwój możliwości odparcia ewentualnego cyberataku oraz minimalizacji jego skutków należy oprzeć na współpracy pomiędzy bankami oraz innymi podmiotami mającymi istotny wpływ na przeprowadzanie transakcji za pośrednictwem zdalnych kanałów [Bojanowski 2013].

Generalnie środki zapobiegania cyberprzestępczości można sklasyfikować w trzech grupach. Pierwszą z nich stanowi rozwijanie i stosowanie metod oraz procedur technicznych służących przeciwdziałaniu możliwości dokonaniu za-

Marzec/March 2015 • vol. II, no. 1 ISSN 2353-5601

machu na określone dobro prawne. Drugą metodę stanowi promowanie bezpiecznego korzystania z nowoczesnych technologii opartych głównie na rozwoju samopomocy oraz podejmowaniu działań publicznoprywatnych służących zwiększeniu świadomości użytkowników o zagrożeniach i kosztach powodowanych cyberprzestępczością. Trzecia metoda koncentruje się na rozwijaniu i polepszaniu współpracy pomiędzy organami ścigania, sektorem prywatnym i użytkownikami końcowymi [Siwicki 2013: 80–83].

Z wielu przeprowadzanych na świecie badań konsumentów wynika, że klienci są gotowi korzystać z technologii biometrycznych ze względu na ich prostotę, brak konieczności posiadania przy sobie dokumentów tożsamości, kart, pamiętania kodów PIN itp. Jednak nadal wyrażają obawy o bezpieczeństwo przechowywanych danych biometrycznych przez instytucję, nawet cieszącą się takim zaufaniem jak bank. Przy przeciwdziałaniu fraudom banki mogłyby wspólnie użytkować rozwiązania biometryczne, obniżając koszty wdrożenia systemu. Byłoby to zgodne z zasadą niekonkurowania i jednocześnie współpracy, gdy chodzi o zapewnienie bezpieczeństwa [Szatkowski 2014].

Przeciwdziałanie nadużyciom zewnętrznym i wewnętrznym w sektorze bankowym jest dużym wyzwaniem organizacyjnym i technologicznym. Nie bez znaczenia jest tu wsparcie ze strony IT. Ograniczając fraudy, obniża się zarówno koszty, jak i straty banku. Trudno dziś wyobrazić sobie funkcjonowanie dużej zaawansowanej technologicznie instytucji finansowej bez wsparcia ze strony takich technologii. Nowoczesny system *fraud detection* powinien na bieżąco uczyć się i dostosowywać do sposobów działania przestępców. To jedna z cech wyróżniających kdprevent™ [*Bezpieczeństwo w instytucji finansowej*..., 2014].

Rozwiązanie kdprevent™ umożliwia tworzenie indywidualnie dostosowanych mechanizmów monitorujących zachowania klientów oraz wykrywanie w tych zachowaniach anomalii. Podstawą są dane o transakcjach, dane osobowe klientów banku, produkty, konta itp. System ma wbudowaną bazę BIZBCB (Baza Incydentów Zagrażających Bezpieczeństwu Czynności Bankowych) oraz wykrywa nietypowe, wcześniej nieobserwowane schematy operacji wykonywanych przez pracowników lub klientów banku. Dzięki temu można prowadzić analizę zachowań: klientów, pracowników, kont i innych ważnych obiektów biznesowych, monitorować płatności w czasie rzeczywistym, jak również wykrywać schematy prania pieniędzy i przeciwdziałać im [*Bezpieczeństwo w instytucji finansowej*..., 2014].

W zależności od instytucji, przeciwdziałanie fraudom może być zorganizowane w bardzo różny sposób. Do podstawowych elementów zarządzania ryzykiem nadużyć zalicza się wewnętrzną politykę firmy w tym zakresie wraz z określonymi procedurami, jednostki realizujące politykę oraz narzędzia, jakimi się one posługują np. Fraud Detection Systems, narzędzia statystyczne etc [Wójcik 2011].

Marzec/March 2015 • vol. II, no. 1 ISSN 2353-5601

W wielu instytucjach finansowych praktykowany jest model organizacyjny, w którym dominuje podejście produktowe. Przykładowo, jeden zespół zajmuje się detekcją i monitoringiem fraudów kartowych w ramach działu operacji, inny fraudami kredytowymi w ramach działu ryzyka lub działu kredytów, a jeszcze inny odpowiada za bezpieczeństwo transakcji w kanałach bankowości internetowej. W takim modelu brakuje pełnej analizy relacji na linii klient–bank, co może prowadzić do zmniejszenia efektywności zespołów poprzez dużą ilość fałszywych alertów. Możliwy jest także jeszcze inny model, w którym zarządzanie ryzykiem nadużyć mieści się w kompetencjach jednej dedykowanej komórki organizacyjnej. Odpowiada ona za zdefiniowanie zjawiska fraudów i tworzenie polityki zarządzania ryzykiem nadużyć, którą objęty jest cały bank. Taki dział odpowiada za obszar nadużyć kredytowych, pracowniczych, kartowych, w bankowości internetowej i obszarze ryzyka operacyjnego. Identyfikuje także nowe obszary zagrożeń oraz bierze udział w ocenie ryzyka wdrażanych produktów, planów sprzedaży i procedur [*Bezpieczeństwo w instytucji finansowej*..., 2014].

Wsparcie organów ścigania państw członkowskich UE w zakresie zwalczania przestępczości elektronicznych instrumentów płatniczych leży w zakresie kompetencji zespołu operacyjnego (Focal Point) terminal. FP Terminal funkcjonuje w strukturze Europolu od 2003 r. i dotychczas jego działania koncentrowały się głównie na zwalczaniu przestępczości bezgotówkowych instrumentów płatniczych przy transakcjach kartowych i bankomatowych. W Europolu zespół funkcjonował początkowo w strukturze Wydziały Ekonomicznego, a następnie, do 2012 r., Wydziału zwalczania fałszerstw pieniądza. Aktualnie, w związku z rosnącym zagrożeniem przestępczymi transakcjami internetowymi, nacisk położony został na zwalczanie przestępczego pozyskiwania danych finansowych, włamania do baz danych, *phising*, dystrybucję danych finansowych w Internecie oraz nielegalne płatności elektroniczne [Skowronek 2013: 126–127].

PODSUMOWANIE

Reputacja w sektorze bankowym ma wartość niemożliwą do przecenienia bowiem z definicji przyjmuje się iż bank jest bezpiecznym miejsce dla powierzenia pieniędzy. I tu wydaje się, że jest miejsce dla bardziej aktywnej roli UKNF, która w ocenie ryzyka operacyjnego powinna pochylić się nad aspektem ryzyka reputacyjnego w kontekście zagadnień, jakie zostały poruszone na III Kongresie Antyfraudowym [*III Kongres antyfraudowy*..., 2012: 10].

Większość instytucji finansowych poniosła znaczne nakłady inwestycyjne w produkty i procesy służące identyfikacji i prewencji „fraudów" w podziale na produkty i kanały sprzedaży (krótki i długi). W nowoczesnych technologiach informatycznych widoczne jest zintegrowane podejście do walki z wyłudzeniami, pozwalające na automatyczne dzielenie się informacjami o fraudach w po-

Marzec/March 2015 • vol. II, no. 1 ISSN 2353-5601

dziale na produkty, procesy i kanały sprzedaży [*III Kongres antyfraudowy...*, 2012: 10].

Wyłudzenie wewnętrzne (internal fraud) jest endemicznie przypisane instytucjom finansowym. Banki i inne instytucje finansowe – zwłaszcza o zasięgu międzynarodowym – powinny posiadać w swych strukturach wyodrębnione i wyspecjalizowane komórki organizacyjne „antyfraudowe". Ważne jest również, aby UKNF nadał odpowiednią wagę w ocenie skuteczności zarządzania ryzykiem operacyjnym rozwiązaniom prewencji antyfraudowej [*III Kongres antyfraudowy...*, 2012: 10].

Wykorzystanie technologii w sektorze usług finansowych, dało ogromny impuls do rozwoju. Jednakże, ze względu na duże uzależnienie od elektronicznych i cyfrowych narzędzi do przeprowadzania transakcji handlowych oraz płatności, występuje poważne zagrożenie bezpieczeństwa i niezawodność operacji finansowych. Wraz z rosnącą tendencją on-line i cybertransakcji, liczba oszustw bankowych dotyka coraz większej liczby osób korzystających z bankowych narzędzia technologii. Oszustwa w płatnościach on-line, bankomatów, kart elektronicznych i transakcji bankowych netto stały się poważnym problemem. Ogromna strata pieniędzy ludzi i instytucji jest spowodowana co roku z powodu tych nadużyć w cyberprzestrzeni w bankach, nawet przy dużych środkach bezpieczeństwa transakcji elektronicznych [Soni i Soni 2013: 22].

BIBLIOGRAFIA

III Kongres antyfraudowy – podsumowanie z debaty kongresowej, 2012, Warszawa, [w:] https://www.kpf.pl/ pliki/iiikaf/podsumowanie.pdf.

Adamski A., 2000, *Prawo karne komputerowe*, Wydawnictwo C. H. Beck, Warszawa.

Bezpieczeństwo w instytucji finansowej: kdprevent – pewna historia o nadużyciach, 2014, „Bank", nr 04.

Bojanowski J., 2014, *Podatność banków na cyberprzestępczość – ćwiczenia Cyber-EXE Polska 2013*, XIV seminarium w cyklu Informatyka w instytucjach finansowych. Fraudy bankowe i ubezpieczeniowe – przeciwdziałanie i wykrywanie poprzez informatykę.

Góra J., 2014, *Dobre Praktyki w zakresie pozyskiwania i gromadzenia elektronicznego materiału dowodowego*, XIV seminarium w cyklu Informatyka w instytucjach finansowych. Fraudy bankowe i ubezpieczeniowe – przeciwdziałanie i wykrywanie poprzez informatykę.

http://finansopedia.forsal.pl/wiki/Fraud.

Jaroch W., 2013, *Zagrożenia systemu bankowego jako kategoria przestępczości gospodarczej*, [w:] *Zagrożenia w sektorze bankowym. Analiza kryminalna zjawisk oraz możliwości przeciwdziałania*, red. P. Chlebowicz, Katedra Kryminologii i Polityki Kryminalnej, Olsztyn.

Liszkiewicz M., 2014, *Przestępstwa komputerowe przeciwko ochronie informacji – zapobieganie i zwalczanie przy zastosowaniu metod i technik informatyki śledczej*, XIV seminarium w cyklu Informatyka w instytucjach finansowych. Fraudy bankowe i ubezpieczeniowe – przeciwdziałanie i wykrywanie poprzez informatykę.

NBP, 2014, *Ocena funkcjonowania polskiego systemu płatniczego w II półroczu 2013 r.*, Warszawa, [w:] http:// www.nbp.pl/systemplatniczy/ocena/ocena2013_2.pdf.

Marzec/March 2015 • vol. II, no. 1 ISSN 2353-5601

NBP, 2013, *Porównanie wybranych elementów polskiego systemu płatniczego z systemami innych krajów Unii Europejskiej za 2012 r.*, [w:] http://www.nbp.pl/systemplatniczy/obrot_bezgotowkowy/porownanie_UE_ 2012.pdf., grudzień.

Piołunowicz M., 2006, *Kategoryzacja strat operacyjnych w bankowości*, „Bank i Kredyt", nr 9.

Prawie 1% rocznych przychodów sklepów internetowych pochłaniają fraudy!, [w:] http://www.handelinternetowy. pl/prawie-1-rocznych-przychodow-sklepow-internetowych-pochlaniaja-fraudy/, dostęp: 17.09.2013.

Rządowy Program Ochrony Cyberprzestrzeni na lata 2011–2016, [w:] http://bip.msw.gov.pl/bip/programy/19057, dok.html.

Siwicki M., 2013, *Cyberprzestępczość*, Wydawnictwo C. H. Beck, Warszawa.

Skowronek M., 2013, *European Cyber Crime Centre (EC3), odpowiedź na zagrożenia wynikające z cyberprzestepczości, ze szczególnym uwzględnieniem zwalczania przestępczości płatności elektronicznych*, [w:] *Przestępczość teleinformatyczna*, red. J. Kosiński, Wydział Wydawnictw i Poligrafii Wyższej Szkoły Policji, Szczytno.

Soni R. R., Soni N., 2013, *An Investigative Study of Banking Cyber Frauds with Special Reference to Private and Public Sector Banks*, „Research Journal of Management Sciences", vol. 2(7), 22–27, July, [w:] http://www.isca.in/IJMS/Archive/v2/i7/4.ISCA-RJMS-2013-062.pdf.

Szatkowski B., 2014, *Bank i Klient: Biometria w polskich realiach*, „Bank" 06.

Uryniuk J., 2011, *Transakcje kartami coraz bezpieczniejsze*, Dziennik Gazeta Prawna, nr 63(2949), 31 marca.

Uryniuk J., *Złodzieje chętniej sięgają nam do kieszeni. Po karty płatnicze*, [w:] http://serwisy.gazetaprawna.pl/finanse-osobiste/artykuly/792575,zlodzieje-chetniej-siegaja-nam-do-kieszeni-po-karty-platnicze.html, dostęp: 24.04.2014.

Witański M, 2014, *Ślady elektroniczne jako elementy informacji zarządczej w bankach i instytucjach ubezpieczeniowych*, XIV seminarium w cyklu Informatyka w instytucjach finansowych. Fraudy bankowe i ubezpieczeniowe – przeciwdziałanie i wykrywanie poprzez informatykę.

Wójcik M., 2011, *Raport specjalny: Oszustwa w banku i ich szacowanie*, „Bank", nr 12.

UNAUTHORIZED BANKING TRANSACTIONS AS A MANIFESTATION OF CYBERCRIME

The development is intended to indicate to one of the key challenges that the banking industry is facing growing cases of bank frauds. Race for supremacy in a comfortable sales – on-line – it becomes an opportunity for criminals to fraud. This means that banks and other financial institutions have in front of you to manage the conflict between its client sales and maintaining its security so that the „convenience" did not become an opportunity for criminals. Hence it is important that the effectiveness of the management of this conflict was perceived by the market regulator.

Key words: frauds, electronic banking, cybercrime.