KOMISJA NADZORU FINANSOWEGO

Zastępca Przewodniczącego
Wojciech Kwaśniak

Warszawa, dnia 15 grudnia 2016 r.

DIB/WPP/711/1/3/2016/IK

Prezesi Zarządów
Banków Komercyjnych

Prezesi Zarządów
Banków Zrzeszających

Prezesi Zarządów
Zrzeszonych Banków Spółdzielczych
za pośrednictwem banków zrzeszających

Spółdzielnia Systemu Ochrony
Zrzeszenia BPS

Spółdzielczy System Ochrony SGB

Krakowski Bank Spółdzielczy

Bank Spółdzielczy w Brodnicy

Krajowa Spółdzielcza Kasa
Oszczędnościowo-Kredytowa

Spółdzielcze Kasy Oszczędnościowo-
Kredytowe
za pośrednictwem **Krajowej Spółdzielczej**
Kasy Oszczędnościowo-Kredytowej

Dyrektorzy Oddziałów Instytucji
Kredytowych

Szanowni Państwo,

W związku z art. 106 ust. ustawy z 29 sierpnia 1997 r. Prawo bankowe (Dz. U. 2016 r., poz. 1988) zobowiązującym banki do przeciwdziałania wykorzystywaniu swojej działalności dla celów mających związek z przestępstwem, o którym mowa w art. 165a lub art. 299 ustawy z dnia 6 czerwca 1997 r. kodeks karny (Dz. U. nr 88, poz. 553, z późn.zm.) oraz art. 106a ust. 1 ustawy Prawo bankowe nakazującym zawiadomienie prokuratora, policji lub innego właściwego organu w razie zaistnienia uzasadnionego podejrzenia, że działalność banku jest wykorzystywana w celu ukrycia działań przestępczych lub dla celów mających związek z przestępstwem skarbowym lub innym przestępstwem niż przestępstwo, o którym mowa w art. 165a lub art. 299 Kodeksu karnego, Urząd Komisji Nadzoru Finansowego (UKNF) zwrócił się do istotnych systemowo banków działających na terenie Rzeczypospolitej Polskiej z pytaniami, których celem było ustalenie zakresu działań podejmowanych, w tym przyjętych mechanizmów kontrolnych zawartych w procedurach

wewnętrznych, w stosunku do powtarzających się przypadków „sprzedaży"[1] w Internecie imiennych rachunków, zazwyczaj wraz z powiązanymi instrumentami płatniczymi i danymi dostępowymi do systemu bankowości internetowej sprzedawanego rachunku.

Informacje uzyskane z badania ankietowego wskazują, że istnieje potrzeba wzmocnienia mechanizmów kontrolnych mających na celu zabezpieczenie instytucji finansowych przed ryzykiem prania pieniędzy oraz finansowania terroryzmu, jak również przed innymi przestępstwami związanymi z nielegalnym obrotem rachunkami.

Pragnę podkreślić, że zjawisko sprzedaży rachunków, jak również funkcjonowania w systemie bankowym tzw. rachunków skompromitowanych wymaga dodatkowych mechanizmów umożliwiających ograniczenie tego ryzyka, poza stosowaniem środków bezpieczeństwa finansowego, o których mowa w art. 8b ust. 1 i ust. 3 ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2016 r. poz. 299, z późn. zm.), jak również implementacji wskazań zawartych w Rekomendacji KNF dotyczącej bezpieczeństwa transakcji płatniczych wykonywanych w Internecie przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo-kredytowe (dalej: Rekomendacja). Należy podkreślić, że rachunki skompromitowane są wykorzystywane nie tylko w celu prania pieniędzy. Ich rolą jest również umożliwienie unikania zajęć komorniczych, ukrywanie dochodów przed organami podatkowymi, przyjmowanie płatności z tytułu sprzedaży nieistniejących produktów na aukcjach internetowych, przekazywanie i wypłacanie środków z innych oszustw i wyłudzeń. Katalog czynów przestępczych, do których wykorzystywane są rachunki skompromitowane jest niezmiernie szeroki.

Mając na względzie, że przedmiotowe zjawisko rodzi istotne implikacje zarówno w sferze ryzyka operacyjnego dla instytucji finansowych prowadzących rachunki, jak i w odniesieniu do zapobiegania wykorzystaniu ich działalności do popełniania przestępstw, w tym prania pieniędzy i finansowania terroryzmu, niniejszym pragnę przedstawić przykłady mechanizmów kontrolnych które mogą przyczynić się do ograniczenia występowania przedmiotowego procederu.

Według informacji zgromadzonych przez UKNF, problematyka sprzedaży rachunków przejawia się głównie w formie udostępniania już założonych rachunków, bądź zakładania rachunków z chwilą, gdy na ogłoszenie o sprzedaży rachunku odpowie zainteresowana osoba. Zgodnie z odpowiedzią ankietowanych banków, to właśnie ta druga forma obrotu rachunkami jest zdecydowanie popularniejsza.

Jako mechanizmy kontrolne w głównej mierze stosowane były przez banki zapisy w regulaminach wskazujące, że przekazanie danych do logowania osobom trzecim stanowi podstawę dla banków do podjęcia działań prewencyjnych takich jak m.in. blokada dostępu do rachunku i zobowiązanie klienta do bezpośredniej interakcji w celu potwierdzenia tożsamości korzystając z fizycznej weryfikacji dokumentów z danymi pozyskanymi podczas nawiązywania relacji.

---

[1] Pojęcie „sprzedaży" rachunków zostało w piśmie UKNF użyte w sposób potoczny, gdyż opisywane praktyki nie stanowią umowy sprzedaży w rozumieniu przepisów prawa – umowa sprzedaży dotyczy rzeczy lub produktu, natomiast w przypadku umowy rachunku nie można zastosować takiego pojęcia.

W przedmiotowych regulacjach, banki zastrzegały również możliwość wypowiedzenia umowy klientowi naruszającemu regulaminy. Mając powyższe na uwadze, instytucje finansowe prowadzące rachunki powinny w umowie rachunku wskazywać na niedopuszczalność przenoszenia lub udostępniania rachunku osobom innym niż posiadacz rachunku bez wiedzy i zgody instytucji finansowej pod rygorem rozwiązania umowy lub wstrzymania świadczenia usług do czasu bezpośredniej, fizycznej weryfikacji tożsamości klienta.

W szczególności, do działań przestępczych wykorzystywane są instytucje finansowe, w których klient może w systemie bankowości internetowej zmienić numer telefonu służący do odbierania SMS-ów z kodami jednorazowymi do autoryzowania transakcji wykonywanych z danego rachunku.
W związku z tym, należy wprowadzić mechanizmy pozwalające na monitorowanie wszelkich zmian numeru telefonu służącego do autoryzacji transakcji oraz podejmować skuteczne działania mające na celu weryfikację zgodności danych właściciela numeru telefonu z danymi osoby zakładającej rachunek, uwzględniające wskazania Rekomendacji KNF. W celu zapewnienia skutecznego systemu przeciwdziałania nieprawidłowościom na rynku finansowym, w szczególności związanym z praniem pieniędzy lub finansowania terroryzmu oraz cyberprzestępczością, banki powinny przekazywać informacje o zidentyfikowanych przypadkach sprzedaży danych dostępowych do rachunków bankowych, bądź zawierania rachunków z wykorzystaniem skradzionej tożsamości, zgodnie z art. 106d pkt 2 ustawy Prawo bankowe, celem umożliwienia innym instytucjom finansowym blokowania dostępu do rachunków osobom, które dopuściły się przedmiotowego procederu.

W ramach działań prewencyjnych wskazane jest również aktywne monitorowanie stron internetowych, na których mogą pojawiać się oferty sprzedaży rachunków lub zawieranie umów z firmami zewnętrznymi, zajmującymi się wyszukiwaniem zagrożeń w sieci. Dobrą praktyką jest również każdorazowy kontakt z administratorem platformy ogłoszeniowej z żądaniem usunięcia zidentyfikowanych ofert sprzedaży rachunków.

Istotnym elementem skutecznego wykrywania procederu sprzedaży rachunków jest włączenie do zakresu aktualnych szkoleń dla pracowników instytucji finansowej zagadnień związanych z opisem procederu i jego mechanizmów, a także sposobu postępowania w przypadku podejrzenia wystąpienia ww. zjawiska.

Przekazując powyższe oczekuję, że informacje wynikające z niniejszego pisma przyczynią się do podjęcia przez instytucje finansowe działań mających na celu stworzenie skutecznego systemu zabezpieczającego przed procederem sprzedaży rachunków imiennych.

Z-ca PRZEWODNICZĄCEGO
Komisji Nadzoru Finansowego

Wojciech Kwaśniak