Sebastian Chorąży
Adwokat

PO PORADĘ
konsultacje prawne online

Warszawa, 23.05.2022 r.

Komisja Nadzoru Finansowego
pismo złożone przez ePUAP

Prezes Urzędu Ochrony Konkurencji i Konsumentów
pismo złożone przez ePUAP

Rzecznik Praw Obywatelskich
pismo złożone przez ePUAP

Petycja

W imieniu własnym na podstawie art. 4 ust. 1 pkt 1) i pkt 2) *ustawy o nadzorze nad rynkiem finansowym (t. j. Dz. U. z 2020 r. poz. 2059)* oraz na podstawie art. 24 ust. 1 w zw. z ust. 2 pkt 2) i pkt 3) *ustawy o ochronie konkurencji i konsumentów (t. j. Dz. U. z 2021 r. poz. 275),* a także na podstawie art. 1 ust. 2 i ust. 3 *ustawy o Rzeczniku Praw Obywatelskich* - w związku z art. 2 ust. 1, ust. 2 pkt 1 i ust. 3 *ustawy o petycjach (t. j. Dz. U. z 2018 r. poz. 870)* – wnoszę do ww. organów o rozważenie podjęcia czynności nadzorczych wobec sektora finansowego, jak również o podjęcie działań służących prawidłowemu funkcjonowaniu rynku finansowego, gdyż obecnie w sektorze tym powszechnie stosowane są praktyki naruszające zbiorowe interesy konsumentów, a także podstawowe uprawnienia konstytucyjne, takie jak prawo do ochrony własności czy do równego traktowania.

Uzasadnienie

W praktyce zawodowej adwokata co raz częściej spotykam się z przypadkami zgłaszania się klientów banków, którzy zostali oszukani metodą *„na telefon z banku".* Metoda ta często przyjmuje formę prawie doskonałą, gdyż klient otrzymujący połączenie telefoniczne - faktycznie na wyświetlaczu swojego telefonu widzi numer telefonu banku, albo wręcz nazwę konkretnego banku. Technika ta ma określenie *spoofing* i jest najpewniej możliwa dzięki zaniechaniom operatorów telefonicznych i niedoskonałości w protokołach sieci telefonii komórkowej[1].

[1] Takie stanowisko prezentują specjaliści np. https://niebezpiecznik.pl/post/spoofing-rozmow-telefonicznych/ (dostęp: 23.05.2022 r.)

Oczywiście technika podszycia się pod infolinię banku nie jest wystarczająca do wypłaty środków z konta bankowego klienta, który odbiera połączenie telefoniczne od oszustów. Przestępcy wykorzystują dodatkowo własne umiejętności psychologiczne, retoryczne, a także doświadczenie, które nabywają wraz z nawiązaniem każdej rozmowy telefonicznej. Nawiązując połączenie telefoniczne przestępcy zaskakują ofiarę sformułowaniem, iż dzwonią np.: *„z departamentu bezpieczeństwa banku, który wykrył, iż na rachunku bankowym klienta próbowano dokonać niezatwierdzonych transakcji wypłaty środków i zmiany hasła"*. Każdy przeciętny człowiek byłby zaskoczony takim telefonem oraz bardzo zaniepokojony, tym bardziej, jeśliby odebrał taki telefon w pracy czy podczas robienia zakupów – co dodatkowo rozprasza ofiarę i uniemożliwia jej skupienie się na rozmowie telefonicznej (występuje presja czasu i miejsca). Przestępcy właśnie na to liczą. Dzięki umiejętności odpowiednio prowadzonej rozmowy najczęściej nakłaniają wówczas klienta banku do niezwłocznej instalacji na swoim telefonie komórkowym określonej aplikacji[2], bądź przesyłają klientowi link do spreparowanej strony internetowej[3]. Dzięki tym zabiegom przestępcy uzyskują dostęp do loginu i hasła do bankowości internetowej ofiary, a z tą chwilą klient najczęściej traci dostęp do konta bankowego, a w konsekwencji swoje pieniądze.

Zachodzi pytanie – dlaczego metoda ta, która jest znana, która opiera się na różnych niedoskonałościach (w tym operatorów sieci komórkowej, banków, ale i samych klientów) – nie została wyeliminowana przez banki, które mają ogromne możliwości finansowe, techniczne i logistyczne. Banki mogłyby bowiem wyeliminować tę metodę poprzez zastosowanie lepszych zabezpieczeń. Brak działań banków w tym zakresie może przyczyniać się do zbiorowego naruszania interesów konsumentów, a także do zaburzenia prawidłowego funkcjonowania rynku finansowego w Polsce. Brak takiego działania, w sytuacji późniejszego obarczania klientów banków tym, że *„dali się wkręcić"* – może naruszać zasady równości wobec prawa[4], a już na pewno narusza bezpieczeństwo ekonomiczne klientów banków, ich własność, za którą banki odpowiadają w sposób szczególny.

Z doświadczenia zawodowego sporządzającego niniejsze pismo wynika, iż przykładowy schemat działania przestępców wygląda w sposób następujący:

- Klient banku instaluje na telefonie komórkowym aplikację poleconą przez przestępców albo uruchamia przesłany mu link do spreparowanej strony internetowej.

  Konsekwencją powyższego jest to, że przestępcy widzą login i hasło do bankowości internetowej, które wpisuje niczego nieświadomy klient banku.

⇩

[2] Najczęściej jest to aplikacja do zdalnego sterowania telefonem albo aplikacja, która przechwytuje wystukiwane znaki na telefonie komórkowym ofiary, czyli de facto przechwytuje login i hasło do bankowości internetowej.

[3] Dzięki spreparowanej stronie internetowej, która w bardzo dobry sposób imituje stronę internetową prawdziwego banku – ofiara dokonuje próby „zalogowania się" do bankowości internetowej, co oczywiście się nie udaje. Jednocześnie wpisany login i hasło są widoczne dla przestępców – co natychmiastowo wykorzystują do zalogowania się na prawdziwej stronie internetowej banku.

[4] Ryzyko i odpowiedzialność jest przerzucana na klientów banków.

- Po zalogowaniu się przez klienta do bankowości internetowej przestępcy dokonują zmiany hasła do bankowości internetowej, a zatwierdzenie tej zmiany jest dokonywane hasłem do logowania[5], bądź odbywa się poprzez zatwierdzenie osobnym hasłem[6], bądź zatwierdzenie odbywa się poprzez metody biometryczne[7].

  Konsekwencją powyższego jest co do zasady poznanie przez przestępców hasła zatwierdzającego transakcje w banku, następnie zmiana hasła do bankowości internetowej, a w dalszej kolejności (najczęściej) utrata przez klienta banku kontroli nad kontem w bankowości internetowej.

⇩

- W dalszej kolejności przestępcy wywołują kolejne dyspozycje na rachunku bankowym klienta, takie jak:
  - Dokonują zmiany dziennych limitów wypłaty środków z rachunku bankowego,
  - Dokonują różnych transakcji na kontach powiązanych – przekazując np. środki z konta oszczędnościowego na rachunek bieżący, do którego przestępcy uzyskali dostęp,
  - Dokonują zaciągnięcia pożyczki *„na jeden klik"*, po czym pożyczka w ciągu kilku minut jest dostępna na rachunku bieżącym, do którego przestępcy uzyskali dostęp i przejęli kontrolę,
  - Wywołują dyspozycję płatności np. BLIK-iem, a pieniądze są wybierane w czasie rzeczywistym przez wspólnika, który znajduje się w dowolnym miejscu w Polsce, przy upatrzonym wcześniej bankomacie (zazwyczaj z dala od kamer i ludzi),
  - Wywołują dyspozycję płatności kartą np. na rachunek bankowy w Revolut lub w innym systemie oferującym natychmiastowe i przede wszystkim globalne usługi finansowe (chodzi o instytucję znajdującą się poza polską jurysdykcją).

  Konsekwencją wyżej wskazanych czynności jest zaciągnięcie na rachunku bankowym klienta pożyczki w kwocie, która jest oferowana przez dużą część banków *„na jeden klik"*, a także wypłacenie wszystkich środków z rachunku bankowego klienta banku. Czynności te mogą trwać krócej niż 15 minut od chwili zmiany hasła.

Należy zauważyć, że dokonanie wyżej wskazanych czynności mogłoby być niemożliwe, gdyby banki wprowadziły dodatkowe zabezpieczenia, które by chroniły klientów banków, którzy w danej chwili stali się podatni na oszustwo. Część z banków w Polsce jednak tego nie robi.

Wobec powyższego, z uwagi na posiadane przeze mnie doświadczenie oraz działanie w interesie ogólnym klientów banków, tj. w interesie publicznym

[5] Którym przestępcy już dysponują.

[6] Które to hasło przestępcy również pozyskują - co w konsekwencji daje przestępcom wiedzę nt. hasła do zatwierdzania innych transakcji na koncie bankowym, jeśli jest inne niż hasło do logowania.

[7] Co się udaje dzięki trwającej rozmowie telefonicznej, w której przestępca wskazuje klientowi banku, że: *"rozpoczął anulowanie dyspozycji zmiany hasła, która została zablokowana wcześniej przez bank, co wymaga teraz potwierdzeniu przez klienta banku".*

– pragnę przekazać do tut. organów pomysły techniczne, jak przeciwdziałać tego typu przestępstwom. Wyrażam jednocześnie nadzieję, że tut. organy, współdziałając ze sobą lub działając niezależnie – przyczynią się do takich zmian w funkcjonowaniu systemu finansowego w Polsce, które realnie zabezpieczą klientów banków przed okradaniem ich z pieniędzy, które są zdeponowane w bankach. Być może niżej wskazane pomysły będą przyczynkiem do wydania nowych rekomendacji, a także do wzmocnienia działalności edukacyjnej w omawianym zakresie.

Przechodząc do rzeczy pragnę wskazać na następujące:

1. **Instalowanie aplikacji przez klientów banków lub klikanie przez nich w spreparowany link.**

   W tym zakresie banki winny kłaść większy nacisk na edukację klientów co do zagrożeń. Klienci powinni otrzymywać realne wskazówki, ostrzeżenia i materiały edukacyjne, które by wyczulały klientów na nowe zagrożenia. Klienci raz na jakiś czas, przed zalogowaniem do systemu bankowości internetowej, powinni akceptować informację o nowych zagrożeniach i wytycznych co do tego, jak ich unikać. Akceptacja powinna mieć charakter realny, tj. taki, że bez zapoznania się z treścią klient nie zaloguje się do systemu (co do zasady). To na bankach powinien spoczywać obowiązek identyfikacji zagrożeń oraz sposobów przeciwdziałania im, gdyż to banki są dostawcami usług o zwiększonym ryzyku.

   Jeśli klient nie będzie chciał zapoznać się z takimi wytycznymi wówczas powinien mieć możliwość odrzucenia zapoznania się z nimi. Bank dochowałby jednak należytej staranności co do tego, żeby realnie umożliwić klientowi zapoznanie się z zagrożeniami, które mogą go dotknąć przy korzystaniu z bankowości internetowej.

   Obecnie istnieje powszechna praktyka, która jest niewystarczająca w tym zakresie. Sprowadza się ona do przekazywania przez banki wiadomości o zagrożeniach w panelu klienta banku lub poprzez wiadomość e-mail. W natłoku wiadomości cyfrowych (w tym od banków) informacje, które nie wymagają pogłębionej interakcji po stronie klienta – są ignorowane (co jest faktem wynikającym z ery cyfryzacji i nadmiaru informacji, a nie, jak można zakładać - ze złej woli klientów banków).

2. **Dokonanie zmiany hasła do bankowości lub dziennych limitów na koncie**.

   W tym zakresie banki powinny dochować szczególnej ostrożności, w szczególności w sytuacji, gdy do zmiany limitów (w górę) dochodzi chwilę po zmianie hasła do bankowości internetowej lub po próbie dokonania zmiany hasła. W sytuacji, gdy dochodzi do zmiany limitów po uprzedniej zmianie hasła (bez względu na to, czy zmiana hasła nastąpiła pięć minut wcześniej, czy dwa miesiące wcześniej) – system bankowości internetowej odnotowując taką dyspozycję powinien generować alert i określone działanie. Dobrym rozwiązaniem byłoby potwierdzenie telefoniczne przez konsultanta banku lub automat (voicebot), po uprzedniej weryfikacji,

że klient w istocie chce dokonać takiej dyspozycji. Korelacja i przebieg ww. czynności winny być istotne dla zabezpieczeń banku, po to, żeby uczynić nieskutecznym odwlekanie przez przestępcę dokonania zmiany limitów.

Drugim zabezpieczeniem powinna zawsze być blokada dokonywania dyspozycji wypłaty środków lub ich przelewu, np. przez dwie godziny od dokonania zmiany hasła w bankowości internetowej czy zmiany limitów wypłaty środków. Ściągnięcie tej blokady powinno być możliwe wyłącznie poprzez potwierdzenie telefoniczne przez konsultanta banku lub automat, po uprzedniej weryfikacji, że klient w istocie chce dokonać wypłaty lub przelania środków (i de facto robi to z własnej woli).

Trzecim zabezpieczeniem powinno być wylogowanie ze wszystkich urządzeń po zmianie hasła, w tym z aplikacji mobilnych.

3. **Wywoływanie różnych dyspozycji na powiązanych rachunkach bankowych.**

Jeśli do takich transakcji dochodzi po zmianie hasła do bankowości internetowej lub próbie jej zmiany lub po zmianie limitów na koncie – system powinien generować alert i określone działanie. Wydaje się, że i tutaj dobrym rozwiązaniem byłoby potwierdzenie telefoniczne przez konsultanta banku lub automat, po uprzedniej weryfikacji, że klient w istocie chce dokonać takich czynności na powiązanych rachunkach bankowych. Czynnikiem wyzwalającym (jednorazowo) powinna być ww. korelacja i przebieg uprzednich czynności dokonanych na koncie.

Brak uprzedniej zmiany hasła do bankowości internetowej lub zmiany limitów byłby częściowo obojętny dla dodatkowych zabezpieczeń, o których mowa w dalszej części, które w części przypadków i tak by uniemożliwiły przestępcom wydanie środków z konta bankowego, z których chcą pobrać środki w ramach ustalonych limitów.

4. **Wzięcie pożyczki *„na jeden klik”.***

Wygoda zaciągania tego typu pożyczek jest istotna dla klientów banków, ale wygoda ta nie powinna narażać klientów na zaciąganie takich pożyczek przez przestępców - na rachunku bankowym klientów banków. Wobec powyższego zaciągnie tego typu pożyczki, która jest przyznawana przez bank z automatu, dzięki uprzedniemu profilowaniu klienta przez bank – zawsze powinna być telefonicznie potwierdzona przez konsultanta banku lub automat, po uprzedniej weryfikacji, czy klient banku w istocie życzy sobie zaciągnięcia takiej pożyczki. System bankowy, jak się wydaje, w szczególności winien wywoływać alert po stronie banku, jeśli klient oczekuje pożyczki bankowej w pełnym oferowanym mu limicie, tym bardziej, jeśli jest to kwota niezaokrąglona. Przeciętny człowiek upraszcza i kategoryzuje bowiem wiedzę i fakty, które ma przyswoić (zwłaszcza na lata, jak to jest przy spłacie pożyczki), a zatem z pewnością łatwiej jest zapamiętać „okrągłą wartość pożyczki”, aniżeli niezaokrągloną jak np. 19.138,74 zł. Tymczasem dla przestępców liczy się czas

oraz maksymalna wartość pieniędzy, którą mogą ukraść – dlatego zaciągają pożyczki w maksymalnej wartości *„na jeden klik”*. Z tych względów powinna być wymagana rozmowa telefoniczna z człowiekiem, który ma największą możliwość wyłapania dobrej albo złej intencji osoby, która wywołała dyspozycję zaciągnięcia pożyczki, w szczególności nietypowej (z perspektywy klienta).

5. **Wywołanie dyspozycji płatności czy przelewu.**

   W sytuacji, gdy dyspozycja wypłaty środków odbywa się zaraz po zmianie hasła lub zmianie limitów na koncie, ale czynności te zostały uprzednio zweryfikowane przez telefoniczną rozmowę z konsultantem banku lub automatem – powinna zostać zrealizowana.

   Jeśli jednak realizacja np. wypłaty środków BLIK-iem okazuje się mieć miejsce w innej lokalizacji niż ta, w której znajduje się telefon z zainstalowaną aplikacją bankową[8] – system bankowy powinien dokonać weryfikacji takiej wypłaty, np. telefoniczną rozmową z konsultantem banku lub automatem. Porównywanie geolokalizacji powinno dziać się z automatu i zawsze – także względem innych transakcji dostępnych na koncie bankowym. Istotne jest, żeby system bankowy zawsze porównywał geolokalizację urządzenia (miejsca), z którego wywołano określoną transakcję – względem miejsca położenia urządzenia, które posłużyło do zatwierdzenia tej transakcji. W większości przypadków będzie to miejsce tożsame, przy czym takie nie będzie, jeśli przestępca bierze w nim aktywny udział.

W świetle powyższych realiów, z którymi mierzą się codziennie oszukani klienci wydaje się, że banki powinny mocniej zadbać o bezpieczeństwo własnych klientów. Technicznie ww. pomysły są możliwe do wdrożenia i nie wymagają nakładów, których banki nie byłyby w stanie pokryć dla bezpieczeństwa własnych klientów, a także dla własnej renomy.

Jednocześnie za niedopuszczalne jawi się to, że część banków działających na polskim rynku dotychczas nie wprowadziła podobnych zabezpieczeń do wyżej wskazanych (choć są chlubne wyjątki). Takie zaniechania po stronie sektora bankowego jest igraniem prawami klientów banków, w szczególności ich własnością. Sytuacje takie mogą naruszać nie tylko zbiorowe interesy konsumentów, ale także oznaczają, że sektor bankowy nie działa w sposób prawidłowy, gdyż zarabia na niedoświadczeniu i braku specjalistycznej wiedzy klientów. To wywołuje ogromne dramaty wielu oszukanych ludzi[9].

Wobec powyższego wyrażam nadzieję, że zgłoszone niniejszą petycją problemy, a także propozycje ich rozwiązania – staną się przyczynkiem do realnych działań w zakresie ochrony interesów polskich klientów banków.

---

[8] System bankowy powinien przyjmować geolokalizację z telefonu, w którym zainstalowana jest aplikacja bankowości internetowej.

[9] Którzy muszą np. udowadniać przed sądem, że to nie oni zaciągnęli pożyczkę „na jeden klik”. Do czasu wyroku – pożyczka jednak jest formalnie wpisana do odpowiednich rejestrów kredytowych – co może uniemożliwiać takiemu klientowi zaciągnięcie pożyczki, której faktycznie potrzebuje.

Jednocześnie w imieniu własnym, mając na uwadze interes moich klientów, którzy mierzą się z tego typu problemami, a także mając na uwadze interes publiczny – oczekuję wszczęcia stosownego postępowania w ramach kompetencji każdego z organów, do którego petycja została skierowana. Zmiana wymaga zaangażowania organów administracji publicznej.

W świetle art. 4 ust. 3 w zw. z art. 8 ust. 1 ustawy o petycjach wyrażam zgodę na ujawnienie na stronie internetowej podmiotów rozpatrujących petycję moich danych osobowych – w związku z zamieszczeniem skanu niniejszej petycji na stronie internetowej każdego z podmiotów.

Informację o sposobie załatwienia petycji wraz z uzasadnieniem proszę przekazać za pomocą środków komunikacji elektronicznej, tj. za pośrednictwem ePUAP lub poczty e-mail.

Z wyrazami szacunku
adw. Sebastian Chorąży