Rekomendacje sektora bankowego dotyczące przeciwdziałania transakcjom oszukańczym

Niniejsze Rekomendacje mają na celu podniesienie bezpieczeństwa konsumentów, korzystających z usług bankowości elektronicznej (dalej: **„Klient"**, **„Klienci"**) w związku ze wzrostem liczby zgłaszanych oszukańczych transakcji płatniczych na przestrzeni ostatnich lat, związanych w szczególności z rozwojem technologicznym oraz migracją transakcyjnej aktywności Klientów z tradycyjnych placówek bankowych do internetowych (dalej: **„Bankowość Internetowa"**) i mobilnych kanałów obsługi Klientów (dalej: **„Bankowość Mobilna"**) (dalej: **„Rekomendacje"**).

Niniejsze Rekomendacje wypracowane zostały przez ekspertów z sektora bankowego przy udziale przedstawicieli Urzędu ochrony Konkurencji i Konsumentów oraz Komisji Nadzoru Finansowego.

Istotnym celem banków musi być zapewnienie bezpieczeństwa środków powierzonych im przez Klientów. Powyższe oznacza, że obowiązkiem banku jest troska nie tylko o konkurencyjność oferty i związanych z nią funkcjonalności, ale również skuteczne identyfikowanie, kwantyfikowanie i mitygowanie ryzyk potencjalnie wiążących się z korzystaniem z tych funkcjonalności przez Klientów. Banki powinny współpracować w zakresie opracowywania wysokich standardów przeciwdziałania transakcjom oszukańczym.

I. Zasady ogólne

1. Rekomendacje należy traktować jako zbiór dobrych praktyk, które stosuje się według zasady proporcjonalności w sytuacjach, w których bank identyfikuje potencjalne, podwyższone ryzyko dokonania transakcji oszukańczych, obciążających rachunki płatnicze Klientów, z wyłączeniem transakcji dokonywanych kartami płatniczymi.
2. Zakres i sposób stosowania Rekomendacji powinien być uzależniony m.in. od wielkości banku, zakresu prowadzonej działalności oraz profilu ryzyka. Każdy z banków wdraża Rekomendacje adekwatnie do swojej sytuacji, tj. indywidualnie identyfikuje ryzyka wskazane w niniejszym dokumencie, bazując na wnioskach wynikających z historycznych doświadczeń instytucji, w tym analizie sekwencji okoliczności i zdarzeń prowadzących w przeszłości do transakcji oszukańczych, zachowań behawioralnych Klientów, etc.

W oparciu o sformułowane wnioski, bank opracowuje indywidualną strategię ograniczenia wystąpienia transakcji oszukańczych oraz wdraża skuteczne w ocenie banku mechanizmy bezpieczeństwa, dążąc do mitygowania tych ryzyk, które przekraczają apetyt na ryzyko banku.

3. Standardem wspólnej troski o bezpieczeństwo Klientów powinna być regularna, wzajemna wymiana informacji o aktualnych zagrożeniach i metodach popełniania przestępstw przeciwko mieniu Klientów oraz dobrych praktykach przeciwdziałania tym zagrożeniom pomiędzy bankami oraz instytucjami płatniczymi.
4. Wdrożenie rozwiązań w zakresie bezpieczeństwa transakcji, w tym rozwiązań zaprezentowanych w Rekomendacjach, nie ogranicza ani nie wyłącza obowiązku dostawcy usług płatniczych do zwrotu kwoty nieautoryzowanej transakcji płatniczej na zasadach wynikających z przepisów prawa.

II. Czynniki ryzyka

Mając na względzie aktualną wiedzę oraz dotychczasowe doświadczenia sektora bankowego, czynności, zlecane przez Klientów w Bankowości Internetowej lub Bankowości Mobilnej, mogące wiązać się z podwyższonym ryzykiem oszustw, to w szczególności:

1. zlecenie zwiększenia limitów transakcyjnych;
2. odblokowanie możliwości dokonywania transakcji niespecyficznych dla danego Klienta;
3. zlecenie zmiany danych użytkownika, w tym zamiany metod komunikacji z bankiem (np. numeru telefonu, adresu e-mail);
4. złożenie dyspozycji przelewu środków pochodzących z tzw. „kredytów na klik"[1], m.in. w przypadkach gdy kredyt został udzielony na wniosek złożony:
   - bezpośrednio lub w niewielkim odstępie czasu od instalacji Bankowości Mobilnej na nieużytkowanym przez Klienta wcześniej urządzeniu,

[1] Wskazać należy, iż kredyty udzielone w oparciu o umowę zawartą bez fizycznej obecności stron, tzw. „kredyty na klik" nie stanowią transakcji płatniczej w rozumieniu ustawy o usług płatniczych. Nie można zatem tego typu czynności bankowych zaliczyć do transakcji oszukańczych, o których mowa w niniejszych Rekomendacjach. Niemniej jednak banki, dostrzegając problem powiązania transakcji oszukańczych z przyjazną Klientowi procedurą udzielania kredytów, w połączeniu z sekwencją zdarzeń wskazaną w rozdz. II ust. 4 kwalifikują dysponowanie środkami pochodzącymi z udzielanych w ten sposób kredytów, jako czynność wymagającą stosowania szczególnych procedur bezpieczeństwa i na potrzeby niniejszych Rekomendacji wprowadzają je do wymienionych w rozdz. II Czynników ryzyka

- po zmianie telefonu zaufanego, danych teleadresowych, numeru kontaktowego, etc.

5. Inne okoliczności i sekwencje zdarzeń, które według historycznych doświadczeń instytucji, mogą wskazywać na ryzyko transakcji oszukańczej.

(dalej: **„Czynniki ryzyka"**)

Przytaczane w Rekomendacjach Czynniki ryzyka nie stanowią katalogu zamkniętego, służą jedynie do określenia przykładowych czynności, które mogą wywoływać podwyższone ryzyko oszustw.

W przypadku Czynników ryzyka, o których mowa powyżej, bank będzie stosował środki zaradcze i dodatkowe mechanizmy bezpieczeństwa.

III. Środki zaradcze, które należy stosować w celu przeciwdziałania transakcjom oszukańczym

Wymienione w Rekomendacji środki zaradcze można ze sobą łączyć, aby uzyskać ich wysoką skuteczność. W odniesieniu do Czynników ryzyka, bank powinien stosować mechanizmy bezpieczeństwa, m.in.:

1. Cooling period

Cooling period - czas, w którym bank, na skutek przeprowadzonej analizy ryzyka wystąpienia transakcji oszukańczej, wyłącza lub opóźnia możliwość korzystania z określonych produktów, funkcjonalności lub usług oferowanych w Bankowości Internetowej lub Bankowości Mobilnej.

Możliwość dokonania przez użytkownika czynności, pomimo objęcia jej cooling period, powinna być dopuszczalna w przypadku zastosowania przez bank, zakończonego pozytywną weryfikacją, dodatkowego mechanizmu bezpieczeństwa, który umożliwi potwierdzenie woli użytkownika do dokonania czynności i zminimalizuje prawdopodobieństwo oszustwa.

2. weryfikacja z wykorzystaniem połączenia telefonicznego

Połączenie z Klientem, zainicjowane przez bank, w celu przekazania informacji o inicjowaniu transakcji lub potwierdzenia woli jej dokonania przez Klienta (autoryzację), np. weryfikacja z wykorzystaniem tzw. *voice code* – polegająca na zainicjowaniu przez bank połączenia telefonicznego podczas którego Klientowi przekazywany jest kod uwierzytelniający, który powinien być wprowadzony przez Klienta w bankowości elektronicznej w celu potwierdzenia zamiaru dokonania czynności.

3. limity transakcji

Domyślne limity transakcyjne Klientów powinny pozostawać na stosunkowo niskim poziomie. Indywidualne limity transakcyjne, powinny odzwierciedlać ich rzeczywiste potrzeby. Bank powinien prowadzić monitoring i analizę transakcji w odniesieniu do określonych grup Klientów i zachęcać ich do obniżania limitów transakcji, jeżeli aktualny limit transakcyjny tych Klientów jest zdaniem banku za wysoki w stosunku do ich potrzeb. Informacje na temat takiej możliwości powinny być ogólnodostępne.

Rozwiązania te należy wdrożyć zarówno dla instrumentów Bankowości Mobilnej jak i Bankowości Internetowej.

4. metody uwierzytelnienia i kaskadowe mechanizmy bezpieczeństwa

Bank stosuje silne uwierzytelnianie Klientów zgodnie z przepisami prawa. Ponadto, w odniesieniu do Czynników ryzyka, bank może stosować kaskadowe mechanizmy bezpieczeństwa. Oznacza to taki dobór metod dodatkowego zabezpieczenia transakcji i Czynników ryzyka, który jest adekwatny do zidentyfikowanego poziomu ryzyka i dostępnych rozwiązań.

5. ograniczanie funkcjonalności Bankowości Internetowej lub Bankowości Mobilnej

Bank powinien umożliwić Klientowi zablokowanie w Bankowości Internetowej lub Bankowości Mobilnej pewnych funkcjonalności, np. możliwości wykonywania przelewów transgranicznych, przelewów na kwoty ponad wskazane przez Klienta limity, etc. Bank powinien w ogólnodostępny sposób informować Klientów o możliwości dokonania takich blokad.

Wycofanie blokady w takim przypadku powinno być możliwe wyłącznie po zastosowaniu przez bank dodatkowego mechanizmu bezpieczeństwa, ograniczającego podatność na oszustwo w określonym kanale.

6. możliwość weryfikacji autentyczności kontaktu inicjowanego przez bank

Bank powinien zapewnić Klientowi możliwość weryfikacji, czy połączenie telefoniczne faktycznie jest inicjowane przez Bank:

- z wykorzystaniem Bankowości Mobilnej, o ile Klient z niej korzysta,
- w inny sposób, w przypadku braku możliwości dokonania weryfikacji w Bankowości Mobilnej.

Bank powinien informować Klientów w sposób ogólnodostępny o możliwości zweryfikowania autentyczności połączenia i zachęcać do takiej weryfikacji.

7. treść komunikatów

Bank w ramach procesu uwierzytelnienia powinien kierować do Klienta komunikaty o prostej i zrozumiałej treści. Dobrą praktyką jest:

- stosowanie prostych i zrozumiałych pojęć, wyraźnie informujących o wykonywanej czynności, takich jak np. *zlecenie przelewu wychodzącego*, zamiast pojęć niejednoznacznych dla Klienta,
- wyraźne wskazywanie kwoty transakcji (w przypadku transakcji na wysokie kwoty bank może również stosować transkrypcję słowną wartości transakcji),
- wskazywanie odbiorcy środków.

8. możliwość szybkiego dokonania zgłoszenia oszukańczej transakcji płatniczej i zastrzeżenia instrumentu płatniczego

Bank powinien udostępnić Klientowi możliwość szybkiego dokonania zgłoszenia zastrzeżenia instrumentu płatniczego oraz podejrzenia transakcji oszukańczej.

Bank powinien dysponować procedurami i narzędziami służącymi bezzwłocznej i adekwatnej reakcji na informacje powzięte w związku z potencjalnym ryzykiem dotyczącym podejrzenia oszukańczej transakcji płatniczej, w tym informacji dotyczących utraty przez Klientów kontroli nad indywidualnymi danymi uwierzytelniającymi.

Bank powinien zapewnić Klientom dedykowaną linię telefoniczną lub udostępnić możliwość dokonania zgłoszenia w Bankowości Mobilnej, Bankowości Internetowej lub na stronie internetowej banku. Zapewnione w ten sposób kanały kontaktu powinny być przeznaczone wyłącznie do obsługi zgłoszeń, o których mowa powyżej. Informacje kontaktowe powinny być w łatwy sposób dostępne dla Klienta.

W miarę możliwości Bank powinien dążyć do opracowania i udostępnienia Klientom w Bankowości Internetowej lub Bankowości Mobilnej funkcjonalności tzw. *„panic buton"* służących do samodzielnego blokowania instrumentów płatniczych.

9. stosowanie systemów biometrii behawioralnej

Bank powinien podejmować działania mające na celu wdrożenie systemu opartego na biometrii behawioralnej, identyfikującego nietypowe aktywności w Bankowości Internetowej

lub Bankowości Mobilnej Klienta na różnych etapach wykorzystywania Bankowości Internetowej oraz Bankowości Mobilnej.