Urząd Ochrony Konkurencji i Konsumentów

DZIAŁANIA OGRANICZAJĄCE RYZYKO WYSTĄPIENIA TRANSAKCJI OSZUKAŃCZYCH

Zalecenia Prezesa UOKiK
dla dostawców usług płatniczych

Warszawa 2024

ZALECENIA PREZESA UOKiK

SPIS TREŚCI

Wstęp

Szybki rozwój i zwiększona dostępność nowych technologii - zwłaszcza urządzeń mobilnych - sprawiły, że znaczną część aktywności konsumenci przenieśli do internetu i aplikacji na smartfony. Oszczędność czasu, większa dostępność, wygoda i łatwość korzystania z usług finansowych niestety idą w parze z szeregiem ryzyk związanych z bezpieczeństwem transakcji i środków zgromadzonych na rachunkach bankowych. To duże wyzwanie, zarówno dla branży handlowej i finansowej, jak i instytucji odpowiadających za bezpieczeństwo i prawidłowe funkcjonowanie rynku.

Doceniamy działania w kierunku zwiększenia bezpieczeństwa transakcji online podejmowane przez dostawców usług płatniczych. Jednocześnie zwracamy uwagę, że ochrona konsumentów na tym rynku wymaga wypracowania spójnych rozwiązań - systemowych i organizacyjnych - które pozwolą przekuć dobre praktyki w rynkowy standard.

Zwiększenie bezpieczeństwa konsumentów korzystających z usług płatniczych wymaga zaangażowania dostawców tych usług w stworzenie katalogu czynników ryzyka i wypracowania odpowiednich środków zapobiegawczych. W tym celu Prezes Urzędu powołał grupę roboczą, w skład której weszli przedstawiciele m.in. Urzędu Komisji Nadzoru Finansowego oraz eksperci z sektora bankowego. Efektem prac jest zbiór zaleceń Prezesa UOKiK przygotowany we współpracy z przedstawicielami rynku usług finansowych dla jego uczestników.

Czynniki ryzyka w usługach płatniczych

Postęp technologiczny spowodował zmianę nawyków finansowych konsumentów. Sprawy, które jeszcze kilka lat temu wiązały się koniecznością wizyty w placówce banku i rozmową z doradcą, teraz załatwiane są online. Jednocześnie konsumenci często są nieświadomi sposobu działania określonych rozwiązań, a co za tym idzie – związanych z nimi ryzyk.

Bezpieczeństwo transakcji online, to wspólny interes dostawców i odbiorców usług płatniczych. Niedopuszczalne jest przerzucenie całej odpowiedzialności w tym zakresie na konsumenta. Należy podkreślić, że to na dostawcach usług spoczywa ciężar wyczerpującego udzielenia klientom informacji na temat transakcji płatniczych, w szczególności dotyczy to informacji o ryzykach. Najważniejszą rolę pełnią tu banki, które jako instytucje zaufania publicznego, powinny w sposób kompleksowy informować klientów o ryzykach. Wyjaśniać sposoby działania oszustów, a także wdrażać środki monitorowania, komunikacji i reagowania na coraz bardziej wysublimowane metody oszustw i kradzieży. Działania te muszą być prowadzone systematycznie i ewoluować równolegle z rozwojem technologii i zmianami nawyków konsumentów. To samo dotyczy katalogu czynników ryzyka i wytycznych, które mają zminimalizować ich wpływ na konsumentów, korzystających z internetowych usług płatniczych.

Wskazany poniżej zbiór czynników ryzyka, czyli funkcji udostępnianych klientom przez dostawców usług płatniczych, które są najczęściej wykorzystywane do dokonywania transakcji oszukańczych, powstał na podstawie analizy skarg skierowanych do UOKiK przez konsumentów. Ponadto w trakcie prac grupy roboczej został uzupełniony o ryzyka, na które wskazywali przedstawiciele dostawców usług płatniczych, w szczególności sektora bankowego.

Dynamiczny rozwój technologii sprawia, że prezentowanej listy czynników wywołujących ryzyka oraz zaleceń nie należy traktować jako katalogów zamkniętych. Wszelkie zidentyfikowane w ramach niniejszego dokumentu czynniki ryzyka i wskazane w nim zalecenia powinny być stosowane i rozwijane przez wszystkich dostawców usług płatniczych.

01

Możliwość samodzielnego zwiększenia limitów transakcyjnych na koncie klienta z poziomu aplikacji mobilnej lub strony internetowej i utrzymywanie przez klientów wysokich limitów transakcyjnych.

Doświadczenia UOKiK wskazują, że w skrajnych przypadkach w wyniku nieautoryzowanych transakcji płatniczych konsumenci tracili całość środków zgromadzonych na rachunkach rozliczeniowych. Taka sytuacja nie byłaby możliwa, gdyby oszuści uprzednio nie dokonali zwiększenia limitów transakcyjnych, wykorzystując dane uwierzytelniające klienta, lub gdyby klienci mieli świadomość ryzyka związanego z utrzymywaniem limitów transakcyjnych na zbyt wysokim poziomie.

02

Możliwość zaciągnięcia zobowiązania finansowego z poziomu aplikacji mobilnej lub strony internetowej.

Uproszczona i tym samym szybsza procedura oceny zdolności kredytowej w przypadku kredytów konsumenckich oferowanych w aplikacji mobilnej lub z poziomu serwisu internetowego (tzw. „kredyty na klik"), jak również sam dostęp do tej funkcji, mogą powodować, że po uzyskaniu nieautoryzowanego dostępu do konta klienta osoba trzecia dodatkowo będzie mogła zaciągnąć zobowiązanie finansowe. W konsekwencji kwota nieautoryzowanej transakcji płatniczej dokonanej przez taką osobę jest znacznie wyższa.

03

Możliwość samodzielnej zmiany danych na koncie klienta, w tym np. zmiany metod komunikacji (np. numeru telefonu, adresu e-mail) lub danych wpływających na ocenę zdolności kredytowej z poziomu aplikacji mobilnej lub strony internetowej.

Możliwość samodzielnego dokonania zmiany danych na koncie klienta może skutkować tym, że osoba trzecia, która weszła w posiadanie indywidualnych danych uwierzytelniających dostęp do serwisu internetowego, może zmienić również np. numer telefonu używany do kontaktu lub uwierzytelniania transakcji. To umożliwi przestępcy dokonywanie kolejnych transakcji bez świadomości konsumenta.

Dodatkowe ryzyko stwarza możliwość zmiany danych mających wpływ na ocenę zdolności kredytowej. W powiązaniu z możliwością zaciągnięcia zobowiązania finansowego z poziomu aplikacji mobilnej lub konta klienta w serwisie internetowym przy minimum formalności, może prowadzić do wyższej kwoty nieautoryzowanej transakcji płatniczej, a w konsekwencji powstania strat przewyższających kwotę środków zgromadzonych na koncie klienta.

04

Możliwość samodzielnego aktywowania dodatkowych funkcji z poziomu aplikacji mobilnej lub strony internetowej.

Analogiczne ryzyko jak w przypadku zmiany danych do kontaktu niesie ze sobą możliwość aktywacji z poziomu strony internetowej lub aplikacji mobilnej niektórych dodatkowych funkcji i usług. Również w tym przypadku osoba trzecia może dokonać ingerencji, która umożliwi jej wytransferowanie środków klienta w sposób utrudniający lub uniemożliwiający ich namierzenie i odzyskanie przez dostawcę usług płatniczych.

05

Możliwość dokonania natychmiastowego przelewu środków.

W przypadku natychmiastowego przelewu dokonanego przez osobę trzecią konsument ma mniej czasu na reakcję – w szczególności jeżeli nie otrzymuje żadnej dodatkowej informacji o takiej transakcji i nie ma świadomości, że została ona w danym momencie zlecona.

06

Możliwość dokonania płatności kartowej bez fizycznego użycia karty, (CNP) niewymagająca silnego uwierzytelnienia klienta (SCA) przez odbiorcę płatności.

Na zwiększenie ryzyka wystąpienia nieautoryzowanej transakcji płatniczej niewątpliwie wpływa brak wymogu zastosowania silnego uwierzytelnienia klienta (SCA). Wystarczy bowiem, że osoba trzecia wejdzie w posiadanie danych widocznych na karcie płatniczej lub kredytowej należącej do konsumenta, aby natychmiast dokonać transakcji kartowej bez fizycznego użycia karty (CNP) bez jego wiedzy.

Zalecenia dla dostawców usług płatniczych

Dostawcy usług płatniczych powinni na bieżąco wdrażać wszelkie niezbędne środki zaradcze, reagując niezwłocznie na pojawiające się zagrożenia. Podejmowane działania mają skutecznie zapobiegać nieautoryzowanym i oszukańczym transakcjom płatniczym. Poniżej prezentujemy przygotowane przez Prezesa UOKiK dla dostawców usług płatniczych zalecenia w zakresie bezpieczeństwa.

1. Monitorowanie transakcji klientów i odpowiednie stosowanie środków technicznych.

Dostawca usług płatniczych powinien na bieżąco monitorować transakcje dokonywane przez klientów, uwzględniając przy tym zwyczaje konsumentów w kontekście korzystania z usług płatniczych.

Szczegółowy zakres i metody monitorowania transakcji powinny być określone przez dostawcę usług płatniczych.

W ramach monitorowania transakcji i doboru adekwatnych zabezpieczeń antyfraudowych powinien brać w szczególności pod uwagę przeciętne wpływy, wydatki i środki zgromadzone na rachunkach środki klientów, jak również wszelkie inne okoliczności, które w ocenie dostawcy usług płatniczych mogą wskazywać na zwiększone ryzyko wystąpienia fraudu.

Na podstawie ustalonych danych, o których mowa powyżej, powinny być definiowane transakcje typowe i nietypowe. W szczególności jako transakcje nietypowe powinny być rozumiane:

a. jednorazowe transakcje, których wysokość odbiega od wysokości przeciętnie dokonywanych przez danego klienta,

b. zbieg transakcji niskokwotowych lub o kwotach przeciętnie dokonywanych przez danego klienta, występujących po sobie w krótkich odstępach czasowych,

c. transakcje dokonywane bezpośrednio lub w krótkim czasie po dokonaniu zmian na koncie klienta,

d. transakcje nietypowe dla danego klienta z innych przyczyn (np. transakcja zagraniczna w sytuacji, w której dotychczas klient takich transakcji nie wykonywał).

Ponadto dostawca usług płatniczych powinien monitorować transakcje, które pomimo że nie muszą zostać uznane za nietypowe, mogą być z innych powodów transakcjami podwyższonego ryzyka, takie jak:

e. transakcje dokonywane w krótkim czasie po aktywacji aplikacji mobilnej - szczególnie jeżeli klient dotychczas nie korzystał z takiej aplikacji, lub nie logował się na konto klienta dostępne z poziomu serwisu internetowego,

f. transakcje dokonywane przez konsumentów, którzy nie wyrazili zgody na objęcie ich ochroną z wykorzystaniem systemów opartych o analizę danych behawioralnych,

g. ciąg zdarzeń wskazujący na to, że sposób dokonania transakcji odbiega od typowo wykonywanych przez danego klienta lub sugerujący schemat oszustwa.

Należy przy tym podkreślić, że wymienione okoliczności stanowią katalog przykładowy i otwarty. Dostawcy usług płatniczych powinni ustalać i modyfikować katalog transakcji uznawanych za nietypowe lub transakcje podwyższonego ryzyka w odniesieniu do danego klienta.

Ustalenie transakcji typowych dla danego klienta ma istotne znaczenie dla zapewnienia równowagi pomiędzy płynnością obrotu, a skutecznością przyjętych rozwiązań i zastosowanych środków technicznych.

2. Cooling period

Cooling period to funkcja opóźniająca wykonanie transakcji od złożenia dyspozycji w systemie przez klienta do czasu jej wykonania przez dostawcę.

Dostawca usług płatniczych powinien stosować cooling period w okolicznościach, w których dokonana przez niego analiza ryzyka lub zalecenia Prezesa UOKiK wskazują, że takie działanie jest zasadne.

Zastosowanie cooling period przy jednoczesnym przekazaniu klientowi stosownej informacji o podstawie do jego zastosowania może w niektórych przypadkach przyczynić się do ograniczenia ryzyka lub uniknięcia wystąpienia nieautoryzowanej transakcji płatniczej. Po otrzymaniu informacji o zastosowaniu cooling period konsument będzie miał odpowiedni czas na weryfikację zlecenia i podjęcie stosownej reakcji.

Z uwzględnieniem ustalonych przez dostawcę usług płatniczych zleceń typowych dla danego klienta wskazane jest stosowanie tego rozwiązania w szczególności w przypadku zleceń/czynności takich jak:

a. istotne lub kolejne podwyższenie limitu transakcji,

b. odblokowanie dodatkowej funkcji dostępnej z poziomu konta klienta w aplikacji mobilnej lub w serwisie internetowym,

c. zmiana danych, w tym zmiana metody komunikacji (np. numeru telefonu),

d. możliwość wypłaty lub dokonania przelewu środków z kredytu w przypadkach, gdy umowa została zawarta poprzez aplikację mobilną lub z poziomu konta klienta w serwisie internetowym,

e. zlecenie dokonania innej transakcji nietypowej dla danego klienta.

Pominięcie cooling period w przypadku transakcji odbiegających istotnie od ustalonego przez dostawcę usług płatniczych profilu transakcji typowej dla danego klienta oraz w przypadku transakcji, która w ocenie dostawcy stanowi transakcję podwyższonego ryzyka, powinno być co do zasady dopuszczalne wyłącznie w przypadkach:

a. zastosowania dodatkowej weryfikacji tożsamości klienta, poprzez inny kanał komunikacji niż ten, w ramach którego klient dokonał polecenia objętego cooling period; w przypadkach, w których zlecenie płatnicze dotyczy wysokiej kwoty lub według dostawcy usług płatniczych dyspozycja budzi podejrzenia z innych powodów, wskazane jest ograniczenie możliwości skrócenia cooling period do złożenia takiej dyspozycji przez klienta w placówce dostawcy usług płatniczych lub zastosowanie innego rozwiązania maksymalnie ograniczającego ryzyko ingerencji osoby trzeciej (np. systemu opartego o biometrię);

b. uprzedniego notyfikowania zamiaru dokonania określonej transakcji przez klienta u dostawcy usług płatniczych (dotyczy transakcji, których kwota przekraczałaby określony poziom).

Dostawca usług płatniczych powinien informować klientów o objęciu danej dyspozycji cooling period.

Istotne, by poza objęciem danej dyspozycji/transakcji/wniosku cooling period dostawca usług płatniczych kierował do konsumenta informację o zleceniu danej operacji i o objęciu jej cooling period.

przykład

Dostawca usług płatniczych odnotował, że w aplikacji mobilnej z konta klienta został złożony wniosek o udzielenie kredytu konsumenckiego („kredyt na klik”). Dostawca stosuje *cooling period*. Powiadomienie o złożeniu wniosku i zastosowaniu cooling period przekazuje konsumentowi innym kanałem, np. telefonicznie. Jednocześnie dostawca wstrzymuje się z wypłatą środków do czasu potwierdzenia przez konsumenta woli skrócenia *cooling period* odrębnym kanałem, np. telefonicznie lub poprzez wygenerowany w aplikacji mobilnej po rozmowie telefonicznej PUSH.

Informację taką konsument powinien otrzymywać co do zasady innym kanałem niż aplikacja mobilna lub konto klienta dostępne z poziomu serwisu internetowego. Najskuteczniejszym rozwiązaniem wydaje się w tym zakresie komunikat voice lub kontakt telefoniczny zainicjowany przez pracownika dostawcy usług płatniczych. W przypadku, gdy w określonym czasie poprzedzającym złożenie: dyspozycji, wniosku lub polecenia transakcji, zmianie uległ kanał komunikacji, dostawca usług płatniczych nie powinien kierować powiadomienia do konsumenta wyłącznie za pośrednictwem tego kanału, który ulegał zmianom, ale również za pośrednictwem innego kanału komunikacji.

Czas *cooling period* nie powinien przekraczać określonych przepisami prawa terminów, w jakich dostawca usług płatniczych jest zobowiązany do wykonania określonej transakcji.

W przypadkach, w których zostanie zastosowany cooling period, i w których po kontakcie z konsumentem dostawca usług płatniczych zostanie poinformowany przez konsumenta o braku autoryzacji takiej transakcji, dostawca usług płatniczych nie może traktować takiej transakcji jako autoryzowanej.

Jeżeli klient wyraził zgodę na aktywację funkcji przelewów natychmiastowych dostawca usług płatniczych co do zasady nie musi stosować cooling period.

Cooling period nie musi również co do zasady być stosowany przez dostawcę usług płatniczych dla dyspozycji zlecanych przez klienta w inny sposób niż na koncie klienta dostępnym z poziomu serwisu internetowego, aplikacji mobilnej lub transakcji CNP, tj. np. dla płatności kartą z fizycznym jej wykorzystaniem lub zleconych przy fizycznej obecności klienta, która umożliwia jego identyfikację.

Cooling period nie musi również być stosowany w przypadku, gdy dostawca usług płatniczych stosuje inny środek o równoważnym lub wyższym poziomie (np. oparty na analizie danych biometrycznych).

3. Komunikaty voice

Dostawca usług płatniczych w określonych sytuacjach, w ramach stosowanych metod uwierzytelnienia, powinien stosować dodatkowo metodę weryfikacji tożsamości polegającą na zainicjowaniu połączenia telefonicznego z klientem, w czasie którego klientowi zostaje przekazana informacja o złożonym z jego konta wniosku, dyspozycji lub zleconej transakcji płatniczej. W trakcie połączenia klient powinien otrzymać kod niezbędny do ukończenia procedury uwierzytelnienia.

Rozwiązanie to powinno być stosowane w szczególności w przypadku dyspozycji lub transakcji, która może być uznana przez dostawcę usług płatniczych za nietypową lub która w ocenie dostawcy stanowi transakcję podwyższonego ryzyka.

4. Limity transakcji.

Sugerujemy, aby limity transakcyjne oferowane domyślnie dla nowych klientów były ustalane na podstawie obiektywnych danych dostępnych dla dostawcy usług płatniczych, np. średniego limitu transakcji dokonywanych przez konsumentów korzystających z danego instrumentu płatniczego. Klienci powinni jednakże nadal mieć możliwość ustalenia limitów transakcyjnych na innym, wybranym przez siebie poziomie. Jednocześnie na etapie zawierania umowy powinni być informowani o ryzykach związanych z utrzymywaniem limitów transakcyjnych na wysokim poziomie.

Również w trakcie trwania umowy dostawca usług płatniczych powinien informować konsumentów za pośrednictwem ustalonych w umowie z klientem kanałów komunikacji o optymalnych limitach transakcyjnych. Ponadto powinien informować o możliwości samodzielnego obniżenia limitów transakcyjnych oraz zachęcać do tego.

Dostawca usług płatniczych powinien ustalić okresy, w jakich będzie dokonywał weryfikacji i korekty rekomendowanych dla klientów limitów transakcji. Okresy te co do zasady nie powinny być dłuższe niż rok.

Istotne podwyższenie limitu transakcyjnego powinno wiązać się z zastosowaniem komunikatu voice lub kontaktem ze strony pracownika dostawcy usług płatniczych z konsumentem, lub inną formą dodatkowego potwierdzenia innym kanałem niż ten, w ramach którego została złożona dyspozycja podwyższenia limitu transakcyjnego.

Granicę, od której zmianę limitu transakcyjnego należy traktować jako „istotną", powinien przy tym ustalać dostawca usług płatniczych, w zależności od okoliczności. W szczególności powinien uwzględnić takie elementy, jak przeciętne wpływy, wydatki i zgromadzone na rachunkach środki danego klienta.

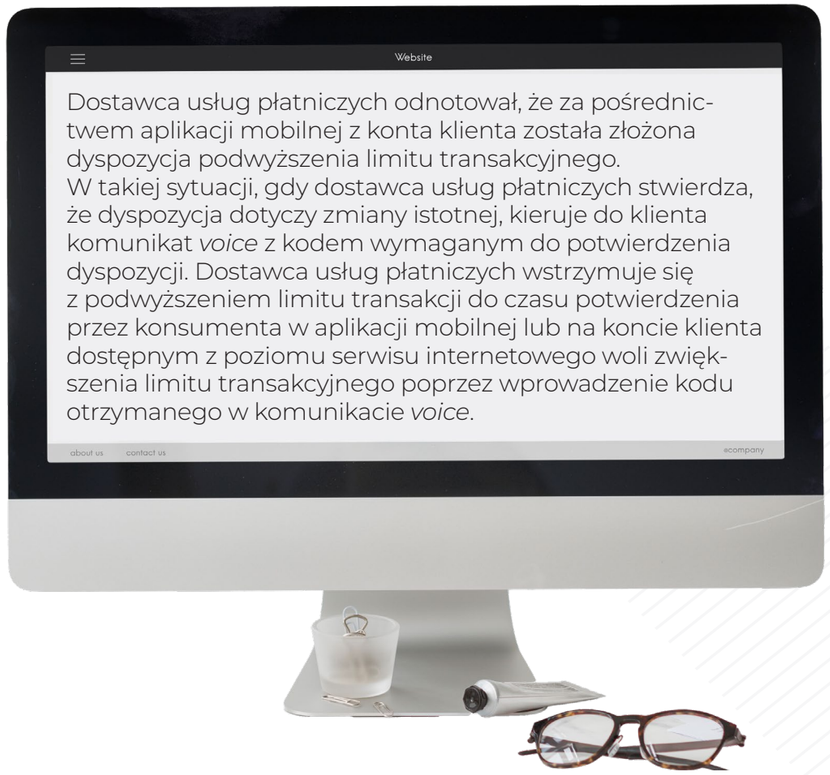
Ponadto w przypadku, gdy następuje próba ponownego podwyższenia limitu w krótkim odstępie czasu – niezależnie od tego, czy zmiana ta jest klasyfikowana przez dostawcę usług płatniczych jako istotne podwyższenie limitu transakcyjnego – dostawca usług płatniczych może zastosować cooling period dla takiej dyspozycji.

W celu zapewnienia konsumentowi maksymalnego bezpieczeństwa i możliwości reakcji na działania, których nie podjął osobiście, informacja od dostawcy

usług płatniczych potwierdzająca złożenie dyspozycji zwiększenia limitów transakcyjnych powinna być kierowana do konsumenta również innym kanałem niż ten, w ramach którego złożył zlecenie. Co do zasady powinien być to również kanał inny niż aplikacja mobilna/konto klienta dostępne z poziomu serwisu internetowego.

W przypadku, gdy w określonym czasie poprzedzającym złożenie dyspozycji zmiany wysokości limitu transakcyjnego zmianie uległ kanał komunikacji, dostawca usług płatniczych nie powinien kierować powiadomienia do konsumenta za pośrednictwem tego kanału, który ulegał zmianom.

przykład



Dostawca usług płatniczych powinien stosować rozwiązanie polegające na tym, że podwyższenie limitów transakcyjnych co do zasady obowiązuje na określony czas, po którym ich wysokość zostaje automatycznie przywrócona do poprzedniej wysokości. Zmiana wysokości limitów transakcyjnych na czas nieoznaczony co do zasady nie powinna być preferowaną ani jedyną opcją oferowaną konsumentom i powinna być dopuszczalna w przypadku dodatkowego potwierdzenia przez konsumenta woli podwyższenia wysokości limitów transakcyjnych na czas nieoznaczony.

5. Ograniczenie niektórych funkcji, w tym dotyczących kredytu konsumenckiego dostępnego z poziomu aplikacji mobilnej lub konta klienta używanego z poziomu serwisu internetowego.

Dostawca usług płatniczych powinien na bieżąco monitorować funkcje i dostępne dla konsumentów produkty, które wykorzystywane są do dokonywania nieautoryzowanych i oszukańczych transakcji płatniczych. Dostawca usług płatniczych nie powinien w przypadku nowo zawieranych umów domyślnie aktywować takich funkcji, przy czym w głównej mierze dotyczy to funkcji dostępnych w aplikacji mobilnej lub na koncie klienta dostępnym z poziomu serwisu internetowego dostawcy usług płatniczych.

Ustalenie katalogu takich funkcji i produktów powinno być dokonywane przez dostawcę usług płatniczych, a także poprzedzone analizą najczęściej występujących schematów oszustw. Wybrane przykłady:

- szybkie przelewy,
- przelewy zagraniczne,
- limit transakcyjny dla transakcji CNP na poziomie powyżej zera.

Dostawca usług płatniczych powinien uzyskiwać od konsumentów osobną wyraźną zgodę na udostępnienie tych funkcji w aplikacji mobilnej na etapie zawierania umowy. Zgoda taka nie powinna być dorozumiana, jednakże procedura jej wyrażenia nie musi być nadmiernie sformalizowana. Istotne, by procedura ta w najwyższym możliwym stopniu ograniczała ryzyko aktywacji takich usług przez osobę trzecią.

Dostawca usług płatniczych powinien jednocześnie na etapie wykonywania umowy umożliwić konsumentom samodzielne ograniczenie wszelkich funkcji, w szczególności tych, o których mowa wyżej. Taka możliwość ograniczenia powinna być dostępna dla klienta w aplikacji mobilnej lub poprzez konto klienta dostępne z poziomu serwisu internetowego - także w sytuacji, w której wyraził on wolę aktywacji tych funkcji konsument na etapie zawierania umowy lub w czasie jej wykonywania.

Każdorazowo przed udostępnieniem funkcji, o których mowa wyżej, dostawca usług płatniczych powinien poinformować klienta o ryzykach związanych z nieautoryzowanym dostępem do konta w aplikacji mobilnej lub w z poziomu serwisu internetowego i ryzykach, jakie wiążą się z wykorzystywaniem określonych funkcji w znanych dostawcy usług płatniczych schematach fraudowych.

Dostawca usług płatniczych powinien jednocześnie na etapie wykonywania umowy umożliwić konsumentom samodzielne ograniczenie funkcji opisanych wyżej, w aplikacji mobilnej, jeżeli uprzednio na etapie zawarcia umowy lub jej wykonywania klient wyraził wolę ich aktywacji.

Aktywacja funkcji uprzednio niedostępnej lub samodzielnie zablokowanej przez konsumenta powinna wiązać się z zastosowaniem cooling period. Ponadto do klienta powinna być kierowana informacja o złożeniu dyspozycji aktywacji danej funkcji. Informacja taka, aby zapewnić skuteczność przyjętego rozwiązania, powinna być kierowana równolegle także innym kanałem niż ten, w ramach którego dokonano zlecenia aktywacji danej funkcji.

W przypadku, w którym w ocenie dostawcy usług płatniczych stosowanie cooling period stanowiłoby nadmierny lub z innych przyczyn nieskuteczny środek, dostawca usług płatniczych powinien zastosować inny środek o równoważnym lub wyższym poziomie (np. oparty na analizie danych biometrycznych).

W przypadku, gdy w określonym czasie poprzedzającym złożenie dyspozycji/wniosku/polecenia transakcji zmianie uległ kanał komunikacji, dostawca usług płatniczych nie powinien kierować powiadomienia do konsumenta za pośrednictwem tego kanału, który ulegał zmianom.

Możliwość zaciągnięcia zobowiązania finansowego – kredytu konsumenckiego – z wykorzystaniem aplikacji mobilnej lub poprzez konto klienta dostępne z poziomu serwisu internetowego (tzw. „kredyt na klik”), nie powinna być domyślnie udostępniana konsumentom. Funkcja ta zawsze powinna być udostępniana na wniosek konsumenta. Dostawca usług płatniczych powinien uzyskiwać od konsumentów osobny, wyraźny wniosek o aktywację powyższej funkcji. Zgoda taka nie powinna być przy tym dorozumiana.

W przypadku złożenia wniosku o udzielenie „kredytu na klik” przez klienta, który tę funkcję aktywował, sugerowane jest, aby dostawca usług płatniczych co do zasady stosował cooling period, albo środek o równoważnym lub wyższym poziomie bezpieczeństwa (np. oparty na analizie danych biometrycznych) w odniesieniu do przyjęcia wniosku do rozpatrzenia lub wypłaty środków na rachunek płatniczy klienta. Rozwiązanie to powinno być stosowane

szczególnie w przypadku, gdy z ustalonego przez dostawcę usług płatniczych profilu klienta wynika, że nie korzystał on dotychczas z podobnych produktów, lub gdy kwota środków, której dotyczy wniosek, jest znacząca w relacji do środków, jakimi obraca dany klient.

Poza objęciem wniosku klienta lub wypłaty środków na rachunek płatniczy rozwiązaniem cooling period albo zastosowaniem środka o równoważnym lub wyższym poziomie bezpieczeństwa (np. opartego na analizie danych biometrycznych) dostawca usług płatniczych powinien kierować do konsumenta informację o fakcie złożenia wniosku o kredyt konsumencki. Informacja taka, aby zapewnić skuteczność przyjętego rozwiązania, powinna być kierowana również innym kanałem niż ten, za pośrednictwem którego złożono wniosek. Dobór odpowiedniego środka, z uwzględnieniem jego ryzyk i ocenianej skuteczności, należy do dostawcy usług płatniczych.

Potwierdzenie wypłaty środków z uzyskanego w ten sposób kredytu również powinno wymagać odrębnego potwierdzenia, złożonego kanałem innym niż ten, za pośrednictwem którego złożył dyspozycję.

przykład

6. Blokada możliwości zalogowania się do aplikacji mobilnej lub konta klienta dostępnego z poziomu serwisu internetowego, jeśli dane urządzenie pozostaje aktywnie połączone sesją zdalną z jakimkolwiek innym urządzeniem.

Dostawca usług płatniczych, biorąc pod uwagę możliwości techniczne, powinien na bieżąco monitorować, czy urządzenia, z których następuje próba logowania do aplikacji mobilnej lub na konto klienta dostępne z poziomu serwisu internetowego dostawcy usług płatniczych, pozostają aktywnie połączone sesją zdalną z jakimkolwiek innym urządzeniem.

W sytuacji, w której dostawca usług płatniczych jest w stanie ustalić, że ma miejsce sytuacja, o której mowa w poprzednim akapicie, powinien zablokować dostęp do aplikacji mobilnej lub na konto klienta dostępne z poziomu serwisu internetowego dostawcy usług płatniczych, w szczególności jeżeli adres IP urządzenia wskazuje na jego lokalizację poza Polską.

Jednocześnie dostawca usług płatniczych powinien kierować do konsumenta informację o fakcie wykrycia i zablokowania takiej próby logowania.

Konsumentowi powinno się umożliwić wyrażenie zgody na logowanie do aplikacji mobilnej lub na konto klienta dostępne z poziomu serwisu internetowego dostawcy usług płatniczych pomimo, że urządzenie pozostaje aktywnie połączone sesją zdalną z innym urządzeniem. Dostawca usług płatniczych powinien przy tym wymagać, żeby w procesie takiego logowania stosować dodatkowe środki bezpieczeństwa.

7. Uwierzytelnienie pracownika dostawcy usług płatniczych.

Dostawca usług płatniczych powinien wprowadzić obowiązek uwierzytelnienia się pracownika przy każdym kontakcie z klientem. Sposób uwierzytelnienia może być uzależniony od funkcji konta dostępnego z poziomu serwisu internetowego lub aplikacji mobilnej.

Uwierzytelnienie się przez pracownika dostawcy usług płatniczych powinno następować automatycznie po zainicjowaniu kontaktu przez dostawcę – nie powinno być uzależnione od żądania klienta.

przykład

Przykłady możliwych rozwiązań:

- ✓ wygenerowanie w aplikacji mobilnej konsumenta komunikatu PUSH i poinformowanie o tym konsumenta w trakcie połączenia,
- ✓ w inny ustalony z klientem sposób (np. z wykorzystaniem ustalonego wcześniej z klientem kodu PIN, hasła lub opisu wzoru graficznego) – jeśli konsument nie korzysta lub dostawca usług płatniczych nie oferuje takiej możliwości w aplikacji mobilnej.

Przykłady wymienione powyżej w punkcie b należy traktować jako katalog otwarty. Wyłącznie od dostawcy usług płatniczych zależy, jakie środki bezpieczeństwa zostaną przez niego zastosowane w przypadku kontaktu z klientami nieposiadającymi lub niekorzystającymi z aplikacji mobilnej.

8. Treść komunikatów kierowanych do klientów.

Wszelkie komunikaty: voice, SMS, PUSH kierowane do konsumentów powinny być zrozumiałe i proste.

W szczególności dotyczy to komunikatów kierowanych do konsumentów w ramach procesu autoryzacji, w których dostawca usług płatniczych powinien:

a. stosować proste i zrozumiałe pojęcia, wyraźnie identyfikujące charakter wykonywanej transakcji, takie jak np. przelew wychodzący, zmiana adresu korespondencyjnego, zmiana kanału komunikacji;

b. stosować krótkie i czytelne objaśnienie charakteru wykonywanej transakcji, w szczególności w przypadku komunikatów SMS lub PUSH w aplikacji mobilnej;

c. w przypadku transakcji kwotowych – określać kwotę transakcji; dla wyższych kwot transakcji może również stosować transkrypcję słowną kwoty;

d. kiedy pozwalają na to możliwości techniczne – wskazywać wyraźnie adresata transakcji.

9. Możliwość odtworzenia treści komunikatów przez klientów.

Wszelkie komunikaty kierowane do konsumentów w ramach procesu autoryzacji powinny być możliwe do odtworzenia przez klienta w każdym momencie przez okres nie krótszy niż 13 miesięcy.

W zależności od możliwości technicznych i funkcjonalności systemów informatycznych dostawców usług płatniczych, komunikaty mogą być udostępniane np. za pośrednictwem aplikacji mobilnej czy konta klienta dostępnego w serwisie internetowym. Jeśli dostawca usług płatniczych nie wykorzystuje w komunikacji z klientami. W sytuacji, w której dostawca usług płatniczych nie stosuje aplikacji mobilnej ani nie oferuje konta klienta dostępnego z poziomu serwisu internetowego, dane takie powinny być niezwłocznie udostępniane na wniosek konsumenta w inny sposób.

Konsument powinien mieć możliwość weryfikacji treści każdego komunikatu, który był do niego kierowany przez dostawcę usług płatniczych, w szczególności:

a. komunikatu w aplikacji mobilnej związanego z uwierzytelnieniem przy wykonywaniu transakcji, składaniu wniosku lub dyspozycji (komunikat PUSH),

b. komunikatu dotyczącego wykonywanej transakcji, składanego wniosku lub dyspozycji kierowanego innym kanałem niż aplikacja mobilna,

c. komunikatu ostrzegającego konsumenta o ryzykach, związanego z nieautoryzowanymi transakcjami płatniczymi kierowanego do klienta w aplikacji mobilnej lub na koncie dostępnym z poziomu serwisu internetowego.

Konsument powinien mieć możliwość nie tylko wglądu do treści komunikatu w aplikacji mobilnej lub na koncie klienta dostępnym z poziomu serwisu internetowego, ale również pobrania jego treści i zapisania na trwałym nośniku.

W przypadku, gdy dostawca usług płatniczych udostępnia konsumentom zarówno dostęp do aplikacji mobilnej, jak i do konta klienta w serwisie internetowym, komunikaty kierowane do konsumenta za pośrednictwem aplikacji mobilnej powinny być również dostępne do wglądu i pobrania z poziomu konta klienta w serwisie internetowym, a komunikaty kierowane za pośrednictwem konta klienta w serwisie internetowym – z poziomu aplikacji mobilnej.

10. Możliwość szybkiego dokonania zgłoszenia nieautoryzowanej lub oszukańczej transakcji płatniczej przez klienta.

Dostawca usług płatniczych powinien wydzielić wyspecjalizowaną, bezpłatną infolinię, jak również czat w aplikacji mobilnej i na stronie internetowej, przeznaczone wyłącznie do obsługi zgłoszeń nieautoryzowanych i oszukańczych transakcji płatniczych.

Dane kontaktowe takiej infolinii powinny być w łatwo dostępne dla konsumentów (brak konieczności przełączania pomiędzy infoliniami). Jednocześnie konsument powinien mieć możliwość wybrania odpowiedniej infolinii w ramach infolinii ogólnej dostawcy usług płatniczych.

Numer infolinii dedykowanej do zgłoszenia nieautoryzowanej lub oszukańczej transakcji płatniczej powinien być uwidoczniony na stronie internetowej dostawcy usług płatniczych, na koncie klienta w serwisie internetowym oraz w aplikacji mobilnej w sposób umożliwiający jego intuicyjne i szybkie znalezienie, ze szczególnym uwzględnieniem osób starszych.

przykład

Przykłady możliwych rozwiązań:

- ✓ wskazanie numeru infolinii do zgłoszenia nieautoryzowanej lub oszukańczej transakcji płatniczej na głównej tablicy na koncie klienta w serwisie internetowym i w aplikacji mobilnej,
- ✓ wskazanie numeru infolinii do zgłoszenia nieautoryzowanej lub oszukańczej transakcji płatniczej w głównym menu na koncie klienta w serwisie internetowym i w aplikacji mobilnej,
- ✓ zastosowanie szaty graficznej ułatwiającej znalezienie wskazanego numeru kontaktowego, np. pogrubiona lub powiększona czcionka, odcinająca się od pozostałej części strony szata graficzna.

Konieczne jest zapewnienie konsumentowi zgłaszającemu nieautoryzowaną lub oszukańczą transakcję płatniczą możliwości obsługi bez nadmiernego czasu oczekiwania na połączenie lub przyjęcie zgłoszenia.

Infolinia przeznaczona do zgłaszania nieautoryzowanych i oszukańczych transakcji płatniczych powinna zapewnić możliwość rozmowy z pracownikiem dostawcy usług płatniczych. Jeśli infolinia obsługiwana jest przez AI lub chatbot – konsument powinien zostać o tym poinformowany w odpowiednim komunikacie na początku rozmowy. Dostawca usług płatniczych powinien przy tym zapewnić konsumentom możliwość przekazania połączenia do konsultanta, o czym konsument również powinien zostać poinformowany. W sytuacji, gdy konsument wyrazi życzenie rozmowy z pracownikiem, powinien zostać niezwłocznie do niego przełączony.

Pracownicy obsługujący infolinię do zgłoszenia nieautoryzowanej lub oszukańczej transakcji płatniczej nie powinni mieć możliwości przełączania klienta na inną infolinię (np. sprzedażową lub obsługę techniczną), o czym konsument powinien być poinformowany na etapie oczekiwania na połączenie lub zaraz po połączeniu.

Jeżeli sprawa, z którą dzwoni konsument, nie dotyczy nieautoryzowanej transakcji płatniczej, połączenie powinno być zakończone przez konsultanta.

11. Przycisk „panic button” / „emergency button”.

Dostawca usług płatniczych powinien udostępnić konsumentowi w aplikacji mobilnej oraz na koncie klienta dostępnym z poziomu serwisu internetowego możliwość natychmiastowej blokady dokonywania jakichkolwiek transakcji - tzw. „panic button”. Funkcja ta powinna być dostępna niezależnie od innych rozwiązań.

Po skorzystaniu przez konsumenta z „panic buton” możliwość dokonywania transakcji powinna pozostać zablokowana do czasu odblokowania jej w placówce dostawcy usług płatniczych lub przez z góry określony czas.

Dostawca usług płatniczych powinien przy tym, natychmiast po zgłoszeniu przez konsumenta nieautoryzowanej transakcji płatniczej lub ryzyka jej wystąpienia, zawiesić możliwość dokonywania transakcji płatniczych z rachunku klienta. Blokada powinna dotyczyć wyłącznie możliwości wykonywania transakcji i nie powinna być powiązana z blokadą kanałów komunikacji dostępnych w aplikacji mobilnej lub na koncie klienta dostępnym z poziomu serwisu internetowego.

12. Stosowanie SCA przy transakcjach CNP w każdym przypadku.

Dostawcy usług płatniczych powinni dążyć do tego, aby w każdym przypadku, w którym konsument zleca dokonanie transakcji kartowej bez fizycznego użycia karty (CNP), wymagane było silne uwierzytelnienie klienta (SCA).

13. Dane uwierzytelniające widoczne na karcie płatniczej.

Dostawcy usług płatniczych powinni dążyć do tego, aby na karcie nie były widoczne dane uwierzytelniające umożliwiające wykonanie transakcji płatniczej z jej wykorzystaniem.

W szczególności dotyczy to numerów CVC/CVV umieszczanych na karcie płatniczej, ponieważ w określonych sytuacjach dane takie mogą być wystarczające do wykonania transakcji.

Rozwiązanie to należy stosować w sytuacji, w której dostawca usług płatniczych nie wymaga SCA w każdym przypadku.

14. Jednorazowe karty wirtualne.

Wskazane jest, aby dostawcy usług płatniczych oferowali klientom możliwość skorzystania z jednorazowych kart wirtualnych, generowanych na potrzeby konkretnej transakcji.

Rozwiązanie to pozwala na minimalizację ryzyka w przypadku wycieku danych uwierzytelniających po stronie odbiorcy płatności, ponieważ nie mogą one zostać ponownie użyte. Jest to również rozwiązanie zabezpieczające konsumentów przed skutkami niechcianych subskrypcji.

Stosowanie tego rozwiązania powinno być przy tym uzależnione od wdrożenia zalecenia, o którym mowa w punkcie 12, tj. wymagania silnego uwierzytelnienia klienta (SCA) w przypadku wszystkich transakcji kartowych niewymagających fizycznego użycia karty (CNP).

15. Klucz sprzętowy U2F.

Dostawca usług płatniczych powinien oferować klientom możliwość skorzystania z metod silnego uwierzytelniania odpornych na przechwycenie sensytywnych informacji przez osoby niepowołane, np. uwierzytelnienie za pomocą kluczy sprzętowych U2F (Universal 2nd Factor), tj. zewnętrznych urządzeń, służących do uwierzytelnienia użytkownika na urządzeniu, z którego zleca on wykonanie transakcji płatniczej.

Ponadto dostawca usług płatniczych powinien informować klientów o zaletach zastosowania takiego rozwiązania, czyli braku możliwości ich wykorzystania przez osoby trzecie, bez fizycznego przejęcia klucza sprzętowego.

16. Stosowanie systemów opartych na sztucznej inteligencji lub biometrii behawioralnej.

Dostawcy usług płatniczych powinni podejmować działania w celu wdrożenia systemów identyfikujących nietypowe aktywności na koncie klienta w serwisie internetowym lub w aplikacji mobilnej na etapie uwierzytelnienia, wykorzystujących sztuczną inteligencję lub biometrię behawioralną.

Stosowanie systemów opartych na gromadzeniu danych behawioralnych powinno przy tym odbywać się:

a. ze wskazaniem rodzaju danych podlegających weryfikacji,

b. wyraźną zgodą konsumentów na przetwarzanie danych tego typu,

c. z jasno ograniczonym celem stosowania pozyskanych danych – tj. tylko w celu weryfikacji prawidłowości uwierzytelnienia,

d. z wyraźnym wskazaniem podmiotów trzecich (w szczególności dostawców systemów) przetwarzających dane osobowe konsumentów.

W przypadku zgody konsumenta na zastosowanie takiego systemu, dostawca usług płatniczych może opcjonalnie ułatwić korzystanie z niektórych funkcji, które domyślnie wymagają dodatkowego lub szczególnego sposobu uwierzytelnienia albo wiążą się z zastosowaniem określonych środków bezpieczeństwa, takich jak np. cooling period.

Uwagi końcowe

Wdrożenie zaleceń nie ogranicza, ani nie wyłącza obowiązków dostawcy usług płatniczych wynikających z innych przepisów, w szczególności ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych, w przypadku zgłoszenia przez konsumenta wystąpienia nieautoryzowanej transakcji płatniczej.

Zalecenia nie wyłączają stosowania innych środków zaradczych i mechanizmów bezpieczeństwa w przypadku pojawienia się czynników ryzyka innych niż wskazane w tym dokumencie. Podobnie jak rozwiązań zapewniających równoważny lub wyższy poziom bezpieczeństwa niż wskazane w tym dokumencie.

Dostawcy usług płatniczych powinni jednocześnie wdrażać wszelkie inne niezbędne środki zaradcze, reagując niezwłocznie na pojawiające się zagrożenia.

Zalecenia mogą podlegać ewaluacji. Dostawcy usług płatniczych, mając na uwadze zidentyfikowane ryzyka, powinni stosować je, aby zapewnić maksymalną skuteczność przyjętej przez nich procedury zapobiegania nieautoryzowanym i oszukańczym transakcjom płatniczym.