Silne uwierzytelnienie – Pytania i odpowiedzi

Zakupy w sklepach stacjonarnych

- **Czy to prawda, że będzie konieczne potwierdzanie PIN-em transakcji także tych nieprzekraczających kwoty 50 PLN?**

Od 14 września kodem PIN trzeba będzie autoryzować również niektóre transakcje na kwoty nieprzekraczające 50 PLN. Banki będą zobowiązane do stosowania tzw. silnego uwierzytelnienia klienta (ang. strong customer authentication, SCA) przy co szóstej transakcji (piąta może być bez SCA) lub jeśli skumulowana wartość transakcji bez silnego uwierzytelniania przekroczy 150 euro. Każda transakcja powyżej 50 PLN, która automatycznie wymaga kodu PIN spowoduje, że licznik transakcji (lub kwoty) będzie startował od początku.

- **Skąd bierze się ta zmiana? Dlaczego będę teraz płacić inaczej?**

Zmiany są efektem nowych przepisów. Nieustający rozwój cyfrowości i pojawiające się nowe rozwiązania w zakresie płatności wymagają jednocześnie nowych zabezpieczeń. Zmiany w sposobie autentykacji płatności wynikają z dyrektywy PSD2, która wprowadza jednolity rynek płatności we wszystkich krajach Unii Europejskiej.

- **W jakich przypadkach/kiedy terminal poprosi mnie o autoryzację transakcji?**

Zależy to od zastosowanego kryterium przez bank-wydawcę karty. Pierwszym z nich jest autoryzacja kodem PIN co szóstej transakcji – o ile wcześniej nie zapłacimy za coś kwoty powyżej 50 PLN, co automatycznie wymaga kodu PIN i zeruje licznik.

Drugie kryterium dotyczy łącznej wartości kolejnych płatności kartą. Gdy przekroczy ona próg 150 euro, autoryzacja PIN-em będzie wymagana. 150 euro jest jednak kwotą maksymalną, a wydawcy kart, czyli przede wszystkim banki, mogą ustalić dla swoich kart próg poniżej 150euro. Jeśli bank zastosuje to właśnie kryterium, to – jak wynika ze statystyk Mastercard –patrząc z perspektywy konsumenta niewiele się zmieni. Zanim bowiem drobne transakcje przekroczą limit 150 euro (ponad 600 PLN), klient statystycznie zrobi transakcję przekraczającą wartość 50 PLN, która i tak wymaga podania kodu PIN.

Każda transakcja z PIN „zeruje licznik" (zarówno w przypadku stosowanego kryterium liczby transakcji, jak i łącznej kwoty transakcji bez SCA).

- **Kto decyduje o tym, jakie kryterium wymogu autoryzacji (liczba transakcji lub ich suma) będzie zastosowane?**

Decyduje o tym wydawca karty. O szczegóły warto więc zapytać w swoim banku/instytucji finansowej.

- **Czy transakcje zliczają się do szóstej w skali jednego dnia/tygodnia, czy też wszystkich transakcji?**

Brane są pod uwagę wszystkie kolejne transakcje poniżej 50 PLN. Przykładowo, jeśli trzy takie transakcje wykonamy w poniedziałek, a dwie we wtorek, to pierwsza transakcja na niską kwotę w środę będzie wymagała autoryzacji kodem PIN. Jednocześnie ta transakcja „zeruje licznik", podobnie jak każda przekraczająca kwotę 50 PLN, która automatycznie wymaga wpisania kodu PIN na terminalu.

- **Chciałbym autoryzować transakcje dokładnie tak samo, jak do tej pory (czyli tylko te przekraczające kwotę 50 PLN). Czy to możliwe?**

Nie, nie będzie to możliwe. Nowe przepisy dotyczą wszystkich użytkowników kart płatniczych.

- **Czy nowe wymogi obowiązują także dla zbliżeniowych płatności mobilnych?**

Tak, silne uwierzytelnienie obejmuje mobilne transakcje zbliżeniowe, gdy cyfrowy odpowiednik karty płatniczej jest zapisany w smartfonie, a płatność jest realizowana za pomocą aplikacji bankowej (standard HCE) lub tzw. portfela mobilnego, takiego jak np. Google Pay.
Nawet jeśli dany portfel mobilny nie stosuje uwierzytelniania dla wszystkich transakcji (za pomocą kodu PIN, odcisku palca itp.), identyfikacja użytkownika przy płatności na kwotę poniżej 50 PLN może być konieczna.

- **Czy przy płatnościach Apple Pay, przy których każda transakcja jest autoryzowana biometrycznie, także będą obowiązywały wymogi z potwierdzaniem PIN-em co szóstej transakcji?**

W przypadku Apple Pay wszystkie płatności są identyfikowane biometrycznie, więc dodatkowe uwierzytelnianie nie jest potrzebne.

- **Czy będą jakieś wyjątki od zastosowania tych wymogów?**

Tak, wyjątkiem zostaną objęte transakcje w samoobsługowych biletomatach (np. w komunikacji miejskiej), parkomatach oraz samoobsługowych bramkach autostradowych.

- **Czy płacąc kartą za granicą będą obowiązywały te same wymogi, co w Polsce?**

Przepisy dyrektywy PSD2 obowiązują tylko w państwach Europejskiego Obszaru Gospodarczego (UE oraz Norwegia, Liechtenstein i Islandia). Poza tym obszarem płatności zbliżeniowe będą działać tak, jak do tej pory.

- **Czy to oznacza, że płatności kartą w sklepie będą teraz bezpieczniejsze?**

Już wcześniej płatności zbliżeniowe były bardzo bezpieczne. Warto wspomnieć, że oferują one wyraźnie wyższy poziom bezpieczeństwa niż te stykowe, a Polska od lat znajduje się na szczycie listy krajów europejskich o najniższej liczbie oszustw kartowych. Niezmiennie posiadacze kart są też chronieni przez rozwiązania technologiczne (np. szyfrowanie danych i standard EMV) oraz przez standardy branżowe i przepisy prawa (np. usługa chargeback, bądź ograniczenie odpowiedzialności posiadacza karty za nieuprawnione transakcje do kwoty 50 EUR w ciągu 24 godzin do zgłoszenia zaginięcia karty). Najnowsze zmiany dodatkowo podnoszą poziom bezpieczeństwa, sprawiając, że nawet gdy karta płatnicza znajdzie się w

niepowołanych rękach, skutki w postaci ewentualnych strat finansowych będą mniej poważne.

- **Czy to oznacza, że płatności kartą w sklepie będą teraz bardziej czasochłonne?**

W doświadczeniu użytkownika zmieni się to, że przy szóstej kolejnej transakcji poniżej kwoty 50 PLN będzie musiał wpisać kod PIN, co trwa maksymalnie kilka sekund. Nie jest to więc zbyt czasochłonne, a z drugiej strony gwarantuje większe poczucie bezpieczeństwa konsumenta. Warto pamiętać, że w 2020 r. limit transakcji bez PIN w Polsce powinien wzrosnąć do 100 PLN. To oznacza, że płatności wymagających podania czterocyfrowego kodu będzie mniej.

Zakupy w sklepach online

- **Jak będą wyglądały płatności kartą online po 14 września 2019 r.?**

Zmiany nastąpią w zakresie autentykacji użytkownika – od tej pory będzie ona musiała być dwustopniowa, czyli obejmować dwa różne elementy opisane w przepisach.

- **Na czym polega tzw. silne uwierzytelnienie klienta?**

Silne uwierzytelnienie klienta polega na weryfikacji co najmniej dwóch elementów należących do trzech kategorii: „wiedza" (co wie posiadacz karty, np. hasło zdefiniowane przez klienta), „posiadanie" (co ma posiadacz karty, np. telefon, na którym znajduje się aplikacja bankowa) i „cechy klienta" (element biometryczny, np. odcisk palca).

- **Kto decyduje o tym, które z tych trzech elementów będę musiał zastosować?**

Będą o tym decydować banki-wydawcy kart. Oczekuje się, że rozwijane będą rozwiązania bazujące na bankowej aplikacji mobilnej i wybranej funkcji biometrycznej. O szczegóły warto zapytać w swoim banku.

- **Jak będzie wyglądać płatność krok po kroku? Czy zawsze tak samo?**

W trakcie płatności online konsument będzie musiał wprowadzić dane swojej karty płatniczej i kliknąć przycisk „Zapłać". W następnym kroku zrealizowane zostanie silne uwierzytelnienie, które może mieć następujący przebieg:
– Użytkownik otrzyma powiadomienie push z aplikacji bankowości mobilnej i będzie musiał wprowadzić swój osobisty kod mPIN lub użytkownik otrzyma powiadomienie push z aplikacji bankowości mobilnej i będzie musiał potwierdzić swoją tożsamość za pomocą odcisku palca lub innych danych biometrycznych.
– Jeśli kod mPIN, odcisk palca (bądź inne dane biometryczne) lub kod jednorazowy SMS zostanie zidentyfikowany pomyślnie, bank zatwierdzi płatność.

- **Mam już kartę z aktywnym rozwiązaniem SecureCode (3D Secure) i korzystam z haseł jednorazowych otrzymywanych w wiadomościach SMS. Czy coś się dla mnie zmieni?**

Zgodnie z nowymi przepisami banki będą mogły oferować identyfikację przez swoją aplikację mobilną, za pomocą odcisku palca lub unikalnego kodu. Jeśli natomiast klient nie ma odpowiedniego urządzenia z aplikacją banku, w dalszym ciągu będzie musiał wprowadzać hasła otrzymywane w wiadomościach SMS, ale będzie też potrzebował dodatkowej metody uwierzytelnienia. Zostanie to określone przez wydawcę karty. O szczegóły warto więc zapytać w swoim banku.

- **Czy każda transakcja online będzie autoryzowana z wykorzystaniem dwóch elementów?**

Z założenia tak, przy czym w kilku przypadkach jest możliwe zastosowanie wyjątków. Mogą one dotyczyć: niskich kwot transakcji (do 50 PLN), płatności cyklicznych (np. abonament za usługi cyfrowe, opłaty za rachunki), wybranych sklepów, którym konsumenci ufają, transakcji o niskim ryzyku oszustwa czy też bezpiecznych płatności korporacyjnych.

- **Kupuję po raz kolejny buty w moim ulubionym sklepie online. Co się dla mnie zmieni po 14 września?**

W przypadku regularnych zakupów u konkretnego sprzedawcy wydawcy kart płatniczych mogą zastosować jeden z wyjątków zdefiniowanych w dyrektywie PSD2. Również sprzedawcy wspólnie ze swoim dostawcą płatności mogą w takich sytuacjach zasugerować bankowi wybrany wyjątek. Decyzja o zastosowaniu wyjątku należy do banku – wydawcy karty, ale informacja od sprzedawcy, że transakcja jest bezpieczna, znacząco zwiększa szansę odstąpienia banku od silnego uwierzytelnienia.

- **Dlaczego potrzebne jest dodatkowe uwierzytelnienie?**

W dobie postępującej cyfryzacji bezpieczeństwo w sieci jest coraz ważniejszą kwestią i dlatego Unii Europejskiej zależy na zwiększeniu bezpieczeństwa płatności i pieniędzy konsumentów. Stąd też dodatkowy element uwierzytelnienia. Zgodnie z wynikami badania Mastercard aż 76% polskich konsumentów uważa, że silna autoryzacja płatności online jest potrzebna, a 28% deklaruje, że dzięki temu będzie częściej robić zakupy w e-commerce.

- **Co jeśli nie mam przy sobie telefonu lub jego bateria się rozładowała?**

W takim przypadku klient nie będzie w stanie przeprowadzić silnego uwierzytelniania, więc płatność online nie zostanie zrealizowana.

- **Czy teraz banki będą częściej proponować rozwiązania biometryczne?**

Banki mają teraz ku temu większe możliwości. Biorąc pod uwagę ich wysoki poziom innowacyjności oraz fakt, że rozwiązania biometryczne są bezpieczniejsze i bardziej wygodne od haseł i kodów, których zdarza się zapominać, możemy się spodziewać popularyzacji tej formy uwierzytelniania w najbliższych latach. W efekcie, biometria pozwoli pogodzić bezpieczeństwo transakcji, którego wymagają przepisy, oraz wygodę i szybkość płatności, których oczekują klienci e-commerce.

- **Jak działają rozwiązania biometryczne? Czy są bezpieczne?**

Rozwiązania biometryczne polegają na identyfikacji fizycznych, unikalnych cech użytkownika, takich jak odcisk palca, zdjęcie twarzy czy skan tęczówki oka. W niedawnym badaniu Mastercard konsumenci uznali, że odcisk palca jest bezpieczniejszą metodą potwierdzania płatności (75%) niż kody jednorazowe (66%), a już niemal połowa ankietowanych (47%) chciałaby w ten sposób uwierzytelniać płatności kartą.

- **Czy to oznacza, że płatności kartą w sieci będą teraz bezpieczniejsze?**

Płatności kartą w internecie już wcześniej były bezpieczne, a korzystając z tej metody płatności konsumenci mogli korzystać m.in. z chargebacku (prawa do reklamacji w przypadku niepowołanej transakcji), czego nie zapewniają inne metody płatności internetowych.
Dodatkowo, ci którzy korzystali z portfeli cyfrowych, takich jak Masterpass, mogli bezpiecznie zapisywać dane swoich kart. Od połowy września dodatkowy poziom bezpieczeństwa, związany z dwuelementową autentykacją, tylko zwiększy naszą ochronę przed oszukańczymi transakcjami.

- **Czy to oznacza, że płatności kartą w sieci będą teraz bardziej czasochłonne?**

Dla części klientów nie zmieni się nic, ponieważ w wielu sklepach płatności są uwierzytelniane przez wydawcę karty np. za pomocą jednorazowego hasła otrzymywanego w wiadomości SMS lub w aplikacji bankowości mobilnej. W efekcie wdrożenia dyrektywy PSD2 wprowadzone zostaną dodatkowe opcje uwierzytelniania, które mogą przyspieszyć ten proces. Tak jest w przypadku uwierzytelnienia biometrycznego, które umożliwia konsumentom potwierdzenie tożsamości przez zwykłe dotknięcie palcem własnego telefonu.