Szanowni Państwo,

uprzejmie informujemy, że zmieniamy sposób potwierdzania płatności kartą w Internecie. Zmiana zostaje wprowadzona zgodnie z Dyrektywą PSD2, zgodnie z którą instytucje finansowe są zobowiązane stosować silne uwierzytelnienie i w przypadku transakcji z użyciem karty, klient będzie zobligowany potwierdzać płatność przy użyciu co najmniej dwóch elementów uwierzytelniania z poniższych kategorii:

- wiedza,
- cechy charakterystyczne użytkownika,
- coś, co posiada użytkownik.

Obecnie przy płatności kartą w Internecie, najczęściej prosimy o potwierdzenie transakcji jednorazowym kodem SMS. To, czy płatność wymaga dodatkowej autoryzacji, zależy od tego, czy sklep internetowy oferuje obsługę płatności z użyciem 3D Secure.

Od 1 sierpnia 2021r. zmieni się sposób potwierdzenia płatności kartą w Internecie.

Usługa silnego uwierzytelnienia opierać będzie się o łączne zastosowanie dwóch czynników:

- kod SMS – element posiadania – bez zmian
- hasło do transakcji internetowych (e-hasło) – element wiedzy – zdefiniowane przez klienta w systemie bankowości elektronicznej e-skok.

E-hasło będzie składało się z 6 znaków. Klient będzie miał możliwość zarówno nadania pierwszego hasła, jak też jego późniejszej zmiany za pośrednictwem systemu bankowości elektronicznej e-skok. **Zastosowany będzie 3 miesięczny okres przejściowy, w którym klient będzie mógł dokonywać transakcji wyłącznie przy użyciu metody SMS do chwili, gdy zdefiniuje w e-skok hasło do transakcji internetowych.** Wraz ze zdefiniowaniem hasła, nastąpi na karcie zmiana metody uwierzytelnienia na SMS + hasło i nie będzie możliwości powrotu do metody SMS. Po upływie okresu przejściowego, nastąpi globalna zmiana metody uwierzytelnienia z SMS na SMS + hasło i od tego momentu żaden klient nie będzie mógł uwierzytelnić płatności przy użyciu jedynie kodu SMS.

Przebieg procesu transakcji.

- Posiadacz w sklepie internetowym wybiera sposób płatności „karta”.
- Posiadacz uzupełnia dane wymagane do transakcji internetowej.
- Akceptant uczestniczący w usłudze 3D Secure przekazuje dostawcy systemu kartowego za pośrednictwem organizacji płatniczej dane transakcji.
- Dostawca systemu kartowego przeprowadza uwierzytelnienie w systemie.
- Dostawca wyświetla zapytanie o e-hasło, a następnie o kod sms.
- Dostawca waliduje poprawność wprowadzonego hasła i sms. Posiadacz/użytkownik będzie miał trzy próby na wprowadzenie e-hasła w trakcie uwierzytelnienia transakcji internetowej, w przypadku wprowadzenia trzykrotnie błędnego e-hasła karta zostanie zablokowana do godz. 23:59. Kartę będzie można odblokować wcześniej kontaktując się z infolinią Centrum Kart SKOK – tak samo, jak w przypadku podania błędnego kodu SMS.

W zależności od specyfiki danego sklepu internetowego przebieg może się nieznacznie różnić, co do zasady jednak w pierwszej kolejności klient będzie proszony o podanie e-hasła, a następnie o jednorazowy kod sms.