Szanowni Państwo,

informujemy, że **od dnia 1 marca 2022r. realizacja transakcji w Internecie odbywać się będzie tylko i wyłącznie z zastosowaniem dwustopniowego uwierzytelnienia tj. e-hasło i jednorazowy kod SMS**.

Zgodnie z dyrektywą PSD II i wdrażającą jej wymagania ustawą o usługach płatniczych, operacje na odległość, w tym transakcje internetowe wymagają tzw. silnego uwierzytelnienia klienta.
Silne uwierzytelnienie klienta (ang. SCA – Strong Customer Authentication) polega na łącznym zastosowaniu dwóch z trzech niezależnych od siebie elementów uwierzytelniających z kategorii:

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

W związku z powyższym **od 1 marca 2022r.** usługa silnego uwierzytelnienia w SKOK 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.

<u>Aby ustanowić/zmienić e-hasło należy:</u>

1. zalogować się do swojej bankowości elektronicznej;
2. w menu głównym wybrać zakładkę „KARTY”;
3. kliknąć przycisk „Ustaw/Zmień e-hasło;
4. wprowadzić nowe e-hasło, składające się z 6 cyfr; jeżeli wcześniej Posiadacz/Użytkownik zdefiniował e-hasło – zostanie ono zastąpione przez aktualnie wprowadzone.
5. zatwierdzić nadanie/zmianę e-hasła kodem SMS (UWAGA! nadanie/zmiana e-hasła jest również silnie uwierzytelniane).

Jeżeli udało się pomyślnie ustawić/zmienić e-hasło, powinien wyświetlić się ekran potwierdzający nadanie nowego e-hasła.

<u>Przebieg procesu transakcji:</u>

- 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 pod numerem 58 511 20 70 – tak samo, jak w przypadku podania błędnego kodu SMS.

Nie zawsze będzie konieczne podawanie e-hasła i kodu SMS – silne uwierzytelnienie nie będzie stosowane między innymi w następujących przypadkach:

- Podczas transakcji cyklicznych – silnego uwierzytelnienia wymaga jedynie transakcja inicjująca płatności cykliczne. Posiadacz uzupełnia dane wymagane do transakcji internetowej.
- Transakcje internetowe wykonane tokenem GPay – od 16 października transakcje te są traktowane przez organizację VISA jako uwierzytelnione – nie będzie konieczności uwierzytelniać ich e-hasłem ani kodem SMS. Dostawca systemu kartowego przeprowadza uwierzytelnienie w systemie.
- Transakcje internetowe, które nie są procesowane w standardzie 3-D Secure – nie wszyscy sprzedawcy stosują standard bezpieczeństwa 3-D Secure.

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.