Toyota
Financial Services

Toyota Bank Polska S.A.

PRZEWODNIK

ZASADY I REKOMENDACJE BANKU DOTYCZĄCE KORZYSTANIA Z SYSTEMU BANKOWOŚCI ELEKTRONICZNEJ

TOYOTA BANK POLSKA S.A.
ul. Postępu 18b, 02-676 Warszawa, toyotabank.pl

Spółka zarejestrowana w rejestrze przedsiębiorców prowadzonym przez Sąd Rejonowy dla m. st. Warszawy, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000051233; NIP: 521-30-92-922; kapitał zakładowy w wysokości 284 163 300 zł, wpłacony w całości.

Toyota Financial Services

Toyota Bank Polska S.A.

SPIS TREŚCI

Toyota Financial Services

Toyota Bank Polska S.A.

1. BEZPIECZEŃSTWO PŁATNOŚCI INTERNETOWYCH W TOYOTA BANK

1.1. TOKEN (KLUCZ)

Do korzystania z serwisu bankowości elektronicznej (internetowej) Toyota Bank wydawał klucz elektroniczny, tzw. token. **Od 19.08.2019 r.** Bank udostępnił nowy system bankowości elektronicznej wraz z aplikacją mobilną do logowania i autoryzacji transakcji. Token będzie mógł być używany dalej **do 13.09.2019 r.** Od **14.09.2019 r.** Toyota Bank planuje całkowite wyłączenie i rezygnację z obsługi tokenów, dlatego prosimy o niezwlekanie z zainstalowaniem i aktywacją aplikacji.

Przed pierwszym logowaniem do bankowości elektronicznej, token należy aktywować łącząc się z Infolinią pod numerem 801 900 700 lub +48 22 488 55 50.

Logując się do serwisu bankowości elektronicznej upewnij się, że robisz to z właściwej strony, tj. https://konto.toyotabank.pl/

Token generuje co minutę unikalny 6-cyfrowy kod, który w połączeniu z indywidualnie ustalonym hasłem umożliwia logowanie oraz autoryzacje zlecanych transakcji. Jeśli nadal korzystasz z tokena pamiętaj, że transakcje w systemie bankowości elektronicznej podpisywane są hasłem i kodem wyświetlanym przez token. Tylko w niżej opisanych sytuacjach system może poprosić o podanie samego kodu z tokena:

a) podczas pierwszego logowania,
b) po odblokowaniu zablokowanego dostępu,
c) po zalogowaniu się tuż przed zmianą kodu wyświetlanego na kluczu.

1.2. HASŁO I TELEKOD

Jeśli nadal używasz tokena, to do korzystania z bankowości elektronicznej wymagane jest indywidualne, ustalane przy pierwszym logowaniu, hasło. Wymyśl trudne i mocne hasło. Bezpieczne hasło powinno się składać z liter i cyfr. Hasło może mieć minimalnie 4 i maksymalnie 8 znaków. Unikaj haseł zawierających łatwe do pozyskania przez osoby trzecie informacje dotyczące Twojej osoby, np. daty Twoich urodzin lub urodzin Twoich bliskich. Dla podniesienia poziomu własnego bezpieczeństwa zmieniaj hasło regularnie, co najmniej raz w miesiącu.

Jeśli chcesz zmienić metodę autoryzacji transakcji w systemie bankowym na aplikację mobilną, to ściągnij aplikację *Mobilna Autoryzacja Toyota Bank*. Następnie przejdź do Systemu Bankowości Elektronicznej i podaj swój identyfikator oraz hasło SMS, które możesz zamówić przez Infolinię (opcja „Aktywuj dostęp do systemu bankowości elektronicznej). Przejdź przez proces aktywacji aplikacji zgodnie ze wskazaniami systemu bankowości i aplikacji mobilnej. Zaloguj się w Systemie Bankowości Elektronicznej swoim identyfikatorem i pierwszym hasłem SMS otrzymanym do aktywacji aplikacji. Zostaniesz poproszony o ustalenie swojego nowego hasła. Twoje hasło musi:

- składać się z minimum 5 i maksymalnie 8 znaków
- zawierać przynajmniej 1 znak specjalny
- zawierać przynajmniej 1 wielką literę
- zawierać przynajmniej 1 małą literę
- zawierać przynajmniej 1 cyfrę

Przy następnym logowaniu do systemu bankowości użyj swojego identyfikatora i ustalonego hasła. Pamiętaj, że zostaniesz poproszony także o zautoryzowanie logowania w aplikacji mobilnej.

Do korzystania z automatycznego systemu telefonicznego (IVR) wymagany jest telekod. Pierwszy telekod otrzymasz SMS-em z banku. Przy pierwszej próbie kontaktu z Doradcą banku zostaniesz poproszony/a o jego zmianę. Telekod składa się z 6 cyfr. Ustaw trudny i unikalny telekod i pamiętaj o jego regularnej zmianie.Autoryzacja klienta w IVR polega na podaniu numeru klienta lub numeru karty i 3-ech losowo wybranych cyfr ustalonego telekodu. System poprosi o podanie całego telekodu jedynie w przypadku nadawania nowego bądź zmiany dotychczas używanego telekodu.

1.3. TWÓJ KOMPUTER I URZĄDZENIE MOBILNE

Zalecane jest korzystanie ze sprawdzonych urządzeń do obsługi systemu bankowości internetowej. Komputery i urządzenia mobilne powinny posiadać legalne oprogramowanie instalowane ze sprawdzonych źródeł. Na urządzeniu powinien zostać zainstalowany dodatkowo program antywirusowy oraz zapora sieciowa (firewall). System operacyjny, oprogramowanie antywirusowe, zapora sieciowa, przeglądarka internetowa powinny być aktualizowane w sposób ciągły. Oprogramowanie, które nie jest na bieżąco aktualizowane, umożliwia łatwiejszą infekcję komputera złośliwym oprogramowaniem.

Nie należy korzystać z niezaufanych urządzeń w celu logowania się do bankowości internetowej.

Nie zaleca się wykorzystywania niezaufanych punków dostępu do sieci w celu połączenia z bankowością np. darmowe Wi-Fi w centrach handlowych, hotelach.

Nie należy przechowywać w sposób niezabezpieczony na komputerze plików z loginami i hasłami, numerami PIN i innymi wrażliwymi danymi. Do tego celu zalecane jest użycie odpowiedniego oprogramowania szyfrującego typu menadżer haseł. Unikaj korzystania z nieznanych komputerów w miejscach publicznych.

1.4. PODEJRZANE WIADOMOŚCI E-MAIL I ZAŁĄCZNIKI

Nigdy nie odpowiadaj na wiadomości e-mail z prośbą o podanie Twoich danych osobowych oraz danych do logowania do bankowości internetowej. Fakt otrzymania takiej wiadomości zgłoś natychmiast do banku. Nie otwieraj załączników w wiadomości e-mail otrzymanej od podejrzanego lub nieznanego nadawcy. Załącznik w takiej wiadomości może zawierać program szpiegujący, który w przypadku otwarcia zostanie niezauważalnie zainstalowany na Twoim komputerze. Oprogramowanie to śledzi Twoje zachowania w internecie i systematycznie przechwytuje istotne informacje oraz przeszukuje zawartość twardych dysków w celu pozyskania danych dotyczących np. kart płatniczych.

Pamiętaj o stosowaniu zaktualizowanych programów antywirusowych i zapory sieciowej (firewall). Minimalizujesz w ten sposób ryzyko zainfekowania Twojego komputera i jego zasobów szkodliwym oprogramowaniem.

1.5. POUFNE INFORMACJE

Zadbaj o poufność wszelkich danych związanych z Twoją bankowością elektroniczną i usługami banku, z których korzystasz. Nie ujawniaj nikomu swojego numeru klienta, hasła, telekodu, numeru i PINu do karty oraz PINu do aplikacji. Jeśli musisz to gdzieś zapisać, zrób w to sposób odczytywalny tylko dla Ciebie (zaszyfrowany) i uniemożliwiający pozyskanie tych danych przez nieuprawnione osoby.

1.6. KARTY PŁATNICZE

Nie ujawniaj nikomu danych Twojej karty, w szczególności daty ważności i numeru CVV (3 cyfry na odwrocie karty). Chroń swój numer PIN. Przed realizacją transakcji wymagającej użycie numeru PIN upewnij się, że nikt go nie podejrzy i nie pozna. Nie przechowuj w tym samym miejscu numeru karty i przypisanego do niej numeru PIN. Jeśli musisz zapisywać takie informacje zadbaj żeby były możliwe do odczytania tylko przez Ciebie, tzn. były zaszyfrowane i odpowiednio chronione.

Pamiętaj, że:

a) PIN do karty możesz nadać i zmienić przez Automatyczny System Telefoniczny;
b) masz możliwość ustalenia indywidualnych limitów na transakcje Twoją kartą (również w internecie), w tym celu skontaktuj się z Infolinią pod numerem 801 900 700 lub +48 22 488 55 50;
c) wszystkie karty debetowe i kredytowe zabezpieczone są mikroprocesorem (technologia EMV);
d) mikroprocesora nie można skopiować;

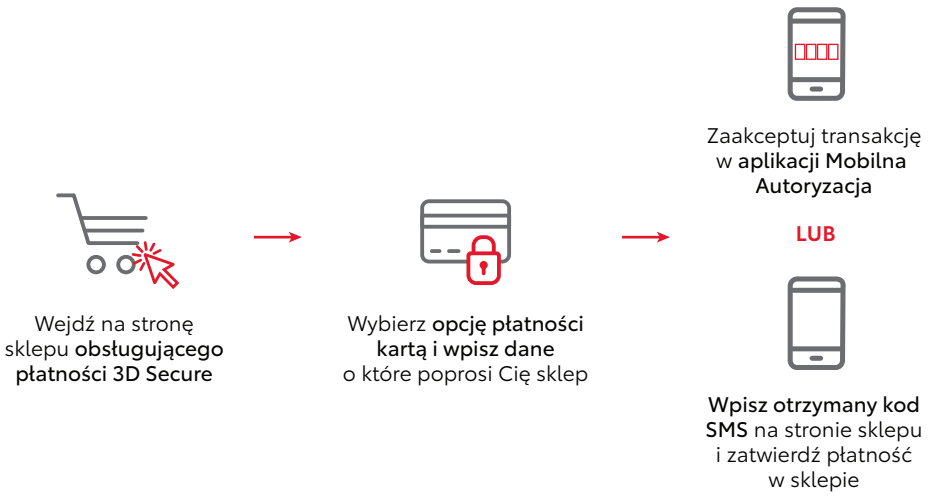
e) nasze karty wyposażone są w bezpieczną technologię płatności zbliżeniowych Pay Wave, co oznacza, że funkcjonalność umożliwiająca ten rodzaj płatności aktywuje się jedynie na 0,5 sekundy w pobliżu czytnika zbliżeniowego, a płatności powyżej 50 zł autoryzowane są standardowo, tj. przez podanie numeru PIN karty.

1.7. 3D SECURE

Jest to dodatkowe zabezpieczenie transakcji kartowych dokonywanych w internecie. Dotyczy wszystkich kart płatniczych Visa wydawanych przez Toyota Bank.

Metoda działania zabezpieczenia jest bardzo prosta i wymaga jedynie dodatkowej autoryzacji transakcji podczas dokonywania zakupów w internecie. Ten mechanizm w znacznym stopniu zwiększa poziom bezpieczeństwa transakcji płatniczych. Dodatkowa autoryzacja polega na:

a) odebraniu komunikatu push na urządzeniu mobilnym z zainstalowaną aplikacją Mobilna Autoryzacja, zalogowaniu się do niej i potwierdzeniu realizacji wykonywanej transakcji lub
b) akceptacji transakcji hasłem SMS otrzymanym podczas wykonywania transakcji



Potwierdzeniem, że sklep internetowy obsługuje standard 3D Secure jest oznaczenie:

Verified by VISA

Podsumowanie:

Usługa 3D Secure to forma dodatkowego zabezpieczenie płatności kartami w internecie z wykorzystaniem dodatkowego potwierdzenia płatności w aplikacji mobilnej lub przy pomocy hasła SMS. Wszystkie karty płatnicze wydane przez Toyota Bank Polska posiadają zabezpieczenie 3D Secure. Zabezpieczenie 3D Secure jest bezpłatne, a jego wyłączenie nie jest możliwe. W przypadku, gdy punkt usługowo-handlowy nie wprowadził wymogu dodatkowej weryfikacji 3D Secure, płatność odbywa się w tradycyjny sposób, a więc bez konieczności dodatkowej akceptacji. Wszelkie problemy z funkcjonowaniem usługi proszę zgłaszać poprzez kontakt z Infolinią Toyota Bank Polska pod numerem 801 900 700; +48 22 488 5550.

1.8. CERTYFIKAT

Komunikacja ze stroną logowania banku (oraz stronami bankowości elektronicznej) zabezpieczona jest certyfikatem. Pozwala on na szyfrowanie komunikacji pomiędzy przeglądarką użytkownika i bankiem. Przeglądarki internetowe pozwalają sprawdzić przez kogo dany certyfikat został wystawiony. Możemy dzięki temu zweryfikować, czy dana strona nie została podmieniona w celu dokonania oszustwa i wyłudzenia np. danych do logowania. Przykładowo używając przeglądarki Mozilla Firefox obok paska adresu możemy kliknąć zieloną kłódkę, następnie klikając „Połączenie" i „Więcej informacji..." Wyświetlone zostaje okienko z zakładką „Bezpieczeństwo". Zobaczyć w nim możemy „Tożsamość witryny", właściciela witryny, czyli w naszym przypadku „Toyota Bank Polska S.A." i witrynę dla której został wystawiony: „konto.toyotabank.pl". Chcąc dokładniej sprawdzić certyfikat należy kliknąć przycisk „Wyświetl certyfikat", pojawi się okienko i dwie zakładki „Ogólne", „Szczegóły" i tutaj również musi się pojawić właściciel „Toyota Bank Polska S.A." i witryna „konto.toyotabank.pl". Należy pamiętać, że certyfikaty posiadają określoną ważność i po jej utracie certyfikat zostaje wymieniony na nowy. Powyższa instrukcja odnosi się do oprogramowania Mozilla Firefox. Jeżeli wykorzystywane są inne przeglądarki np. Microsoft Edge, Opera, Safari, Google Chrome, mamy również możliwość weryfikacji certyfikatów używanych do zabezpieczenia transmisji. Instrukcję możemy znaleźć w dokumentacji odnoszącej się do konkretnej przeglądarki. Zawsze sprawdzaj, czy Twoje programy antywirusowe i zapora sieciowa (firewall) są aktywne, a przeglądarka aktualna. Jeżeli Twoja przeglądarka zachowuje się nietypowo podczas logowania się do lub korzystania z bankowości elektronicznej, zgłoś nietypowe działanie do Banku (0 801 900 700 lub +48 22 488 55 50). Nie korzystaj z bankowości elektronicznej za pośrednictwem niedostatecznie zabezpieczonych urządzeń i sieci internetowych.

1.9. ZASTRZEGANIE DOKUMENTÓW

Toyota Bank uczestniczy w programie Dokumenty Zastrzeżone. Informację o kradzieży lub zagubieniu dokumentów bezzwłocznie przekazujemy do centralnego rejestru.

Jak zastrzec dokumenty?

- zadzwoń na Infolinię pod numer 801 900 700 lub +48 22 488 55 50 (pn-pt. 8-20, sob. 8-14),
- wyślij zgłoszenie przez System Bankowości Elektronicznej,
- skorzystaj z formularza kontaktowego (wymagana zeskanowana dyspozycja z własnoręcznym podpisem).

Poznaj także serwis informacyjny programu Dokumenty Zastrzeżone .

Program prowadzony jest pod patronatem Policji i MSWiA.

1.10. OSTRZEŻENIA I KOMUNIKATY

W zakresie komunikacji nt. poprawnego i bezpiecznego korzystania z usług płatności internetowych wykorzystujemy system bankowości elektronicznej.

Bank przekazuje przez system bankowości elektronicznej informacje o potencjalnych zagrożeniach wynikających z zaobserwowanych działań przestępczych mających na celu przechwycenie danych uwierzytelniających oraz wszelkich innych podejrzanych działaniach mających wpływ na bezpieczeństwo klienta w systemie bankowości elektronicznej.

Informacje dotyczące poprawnego i bezpiecznego korzystania z usług płatności internetowych przesyłane w imieniu Banku innym kanałem niż przez ww. system nie są wiarygodne.

Ten kanał komunikacji może być wykorzystywany również do zgłaszania do Banku wszelkich podejrzanych zdarzeń i nietypowych sytuacji zaobserwowanych w trakcie korzystania z usług banku lub potencjalnych prób wyłudzenia poufnych informacji (np. poprzez e-mail lub telefon) w celu dokonania oszustwa lub uzyskania nieautoryzowanego dostępu do środków zdeponowanych w banku. Bank tym samym kanałem lub w inny, uzgodniony ze zgłaszającym, sposób skontaktuje się i przekaże informacje dotyczące analizy zgłoszenia i dalszych działań podjętych w tym zakresie.

W celu zgłoszenia podejrzanego lub niestandardowego zdarzenia tym kanałem, postępuj zgodnie z poniższą instrukcją:

a) zaloguj się do systemu bankowości elektronicznej korzystają z adresu https://konto.toyotabank.pl/;
b) z menu, dostępnego w lewym górnym rogu, wybierz opcję „Dane i ustawienia", a następnie „Wiadomości";
c) wyświetli się lista Twoich wiadomości. Kliknij przycisk „nowa wiadomość", który znajduję się z prawej strony nad i pod listą wiadomości;
d) wypełnij formularz wiadomości i kliknij „dalej";
e) zweryfikuj treść stworzonej wiadomości i kliknij „wyślij";
f) wysłanie wiadomości zostanie potwierdzone komunikatem „Wiadomość została wysłana";
g) wyloguj się z systemu bankowości elektronicznej.

2. PROCEDURA INICJOWANIA I AUTORYZOWANIA PRZEZ KLIENTA TRANSAKCJI PŁATNICZEJ.

2.1. PRZELEW DOWOLNY NA KONTO W INNYM BANKU

W celu realizacji przelewu na konto w innym banku należy postępować wg poniższej instrukcji:

a) zaloguj się z użyciem identyfikatora klienta i tokena (klucza) lub aplikacji mobilnej w serwisie bankowości elektronicznej pod adresem konto.toyotabank.pl;
b) z menu dostępnych funkcji z lewej strony ekranu lub miniaplikacji na pulpicie systemu wybierz: „Przelewy", a następnie „Wykonaj przelew" i z wyświetlonej listy rozwijalnej wybierz „Zwykły";
c) w wyświetlonym formularzu przelewu należy kolejno:
   - w sekcji „Przelew z rachunku" wybrać konto z którego przelew będzie realizowany (rachunek obciążany)
   - w sekcji „Odbiorca" wybrać właściwego odbiorcę (z listy zdefiniowanych szablonów lub odbiorców) lub uzupełnić to pole i kolejne („Dane odbiorcy" wskazując nazwę skróconą, pełną (wraz z adresem) odbiorcy przelewu
   - w sekcji „Rachunek Odbiorcy" – jeśli nie został wybrany odbiorca lub szablon zdefiniowany należy wpisać pełny 26-cio cyfrowy numer rachunku odbiorcy (NRB)
   - w sekcji „Kwota" wpisać kwotę wykonywanego przelewu, UWAGA – kwota powinna uwzględniać ustawione, przez właściciela konta, wysokości limitów przelewu jednorazowego i dziennego na przelewy realizowane w serwisie bankowości internetowej
   - w sekcji „Tytuł przelewu" wpisać tytuł wykonywanego przelewu
   - w sekcji „Rodzaj przelewu" pozostawić domyślnie zaznaczoną opcję „Zwykły ELIXIR"
   - w sekcji „Data realizacji" pozostawić domyślnie podstawianą bieżącą datę lub kliknąć ikonkę kalnedarza i wybrać inny dzień jeśli przelew ma być wykonany z datą przyszłą
d) po wypełnieniu formularza przelewu należy kliknąć przycisk „dalej";
e) wyświetli się okno z potwierdzeniem realizowanej transakcji wraz z informacjami o terminie i kosztach jej wykonania;

f) jeśli korzystasz z aplikacji Mobilna Autoryzacja Toyota Bank, to wyświetli się komunikat informujący o konieczności autoryzacji przelewu w aplikacji, należy uruchomić aplikację i potwierdzić dyspozycję realizacji przelewu;
g) jeśli nadal korzystasz z tokena, to w sekcji „Podaj hasło i kod z klucza" należy wpisać zdefiniowane hasło i aktualne wskazanie tokena (klucza) i kliknąć „Zaloguj";
h) poprawne zlecenie i potwierdzenie realizacji przelewu zostanie potwierdzone odpowiednim komunikatem;
i) przelew zostanie zrealizowany zgodnie z obowiązującymi w banku godzinami sesji ELIXIR;
j) jeśli w dacie realizacji przelewu została wskazana opcja „dzisiaj", to kwota przelewu automatycznie pomniejszy saldo dostępnych środków na koncie;
k) jeśli w dacie realizacji przelewu została wskazana inna niż domyślnie podstawiona przez system bieżąca data, to kwota tego przelewu pomniejszy saldo dostępnych środków na koncie dopiero w dniu jego realizacji w chwili realizowania przez Bank pierwszej sesji wychodzącej;
l) za realizację przelewu zostanie pobrana opłata zgodnie z aktualną Tabelą Opłat i Prowizji.

Przed potwierdzeniem transakcji zawsze weryfikuj zgodność numeru konta, na które przelewasz środki pieniężne. Jeśli używasz danych odbiorcy zdefiniowanego, to weryfikuj okresowo poprawność danych i czy numery rachunków nie uległy podmianie. Unikaj opcji „kopiuj – wklej" przy uzupełnianiu numeru rachunku odbiorcy Twojego przelewu.

2.2. PRZELEW WEWNĘTRZNY (NA KONTO W TOYOTA BANK)

W celu realizacji przelewu na konto w innym banku należy postępować wg poniższej instrukcji:
a) zaloguj się z użyciem identyfikatora klienta i tokena (klucza)
b) z menu dostępnych funkcji systemu wybierz: „Przelewy", a z wyświetlonej listy rozwijalnej wybierz „Własny ";
c) w formularzu przelewu należy:
- w sekcji „Przelew z rachunku" wybrać konto z którego (obciążany) przelew będzie realizowany
- w sekcji „Na rachunek" wybrać konto na które (uznawany) przelew będzie realizowany
- w sekcji „Kwota" wpisać kwotę wykonywanego przelewu, UWAGA – kwota powinna uwzględniać ustawione, przez właściciela konta, wysokości limitów przelewu jednorazowego i dziennego na przelewy realizowane w serwisie bankowości internetowej
- w sekcji „Tytuł przelewu" wpisać tytuł wykonywanego przelewu
- w sekcji „Data realizacji" pozostawić domyślnie podstawianą bieżącą datę lub kliknąć ikonkę kalendarza i wybrać inny dzień jeśli przelew ma być wykonany z datą przyszłą

d) po wypełnieniu formularza przelewu należy kliknąć przycisk „dalej";
e) wyświetli się okno z potwierdzeniem realizowanej transakcji wraz z informacjami o terminie i kosztach jej wykonania;
f) jeśli korzystasz z aplikacji Mobilna Autoryzacja Toyota Bank, to wyświetli się komunikat informujący o konieczności autoryzacji przelewu w aplikacji, należy uruchomić aplikację i potwierdzić dyspozycję realizacji przelewu;
g) jeśli nadal korzystasz z tokena, to w sekcji „Podaj hasło i kod z klucza" należy wpisać zdefiniowane hasło i aktualne wskazanie tokena (klucza) i kliknąć „Zaloguj"
h) poprawne zlecenie i potwierdzenie realizacji przelewu zostanie potwierdzone komunikatem „Przelew został przyjęty do realizacji";
i) kwota przelewu pomniejszy saldo dostępnych środków na koncie, z którego jest realizowany przelew w dacie zdefiniowanej w sekcji „Data realizacji";
j) za realizację przelewu zostanie pobrana opłata zgodnie z aktualną Tabelą Opłat i Prowizji.

2.3. PŁATNOŚĆ KARTĄ W INTERNECIE

Pamiętaj, że masz możliwość ustalenia indywidualnych limitów na transakcje realizowane w internecie. W tym celu skontaktuj się z Infolinią pod numerem 801 900 700 lub + 48 22 488 55 50.

W celu dokonania płatności kartą w internecie należy podać:
a) dane personalne (imię, nazwisko i miejsca zamieszkania);
b) pełny numer karty;
c) datę ważności karty;
d) 3-cyfrowy kod CVV, który znajduje się na rewersie karty, obok miejsca na podpis.

Po zatwierdzeniu danych, nastąpi realizacja transakcji.

W przypadku, gdy punkt usługowo-handlowy stosuje wymóg dodatkowej weryfikacji transakcji 3D Secure postępuj zgodnie z instrukcją opisaną w punkcie 1.7 niniejszej instrukcji. Wszelkie problemy z realizacją transakcji oraz usługą 3D Secure należy zgłaszać poprzez kontakt z Infolinią Toyota Bank Polska pod numerem 801 900 700; +48 22 488 5550.

2.4. PŁATNOŚĆ ZA POMOCĄ SZYBKIEGO PRZELEWU „ONLINE" (TOYOTA PAY WAY)

Robiąc zakupy w sklepach internetowych możesz również za nie zapłacić za pomocą tzw. szybkiego przelewu online wykorzystując usługę Toyota Pay Way. Tę usługę udostępniamy naszym klientom wspólnie z:

a) Bluemedia;
b) Dotpay;
c) e-Card;
d) Krajowy Integrator Płatności (T-Pay).

Sklepy i serwisy obsługiwane przez ww. firmy udostępniają możliwość zapłaty za zakupione tam towary i usługi szybkim przelewem. Jeśli chcesz zapłacić w ten sposób za zakupy, wystarczy po zakończeniu zakupów wybrać opcję „szybka płatność" lub „płatność online" itp., a następnie kliknąć opcję „Pay Way Toyota Bank", lub w logo Pay Way Toyota Bank. Zostaniesz przeniesiony na stronę logowania do bankowości elektronicznej Toyota Bank. Po zalogowaniu się do serwisu wyświetli się formularz, w którym wszystkie dane identyfikujące Twoją płatność i przelew są wypełnione automatycznie. Po zatwierdzeniu transakcji tokenem lub aplikacją mobilną przelew trafi na konto sklepu i jednocześnie otrzymasz komunikat o prawidłowym dokonaniu płatności. To wszystko. Szybka płatność zrealizowana, a sklep dzięki temu będzie w stanie szybciej wysłać do Ciebie zamówiony towar lub usługę.

Pamiętaj również, że liczba tego typu transakcji jest nieograniczona, a przelewy są darmowe. Kwota płatności zrealizowanych w ten sposób obciąża ustawiony limit transakcji zlecanych przez bankowość internetową. Upewnij się, że po zakończonej transakcji zostałeś/aś wylogowany/a automatycznie z serwisu bankowości internetowej. Jeśli z różnych przyczyn to nie nastąpiło, to wyloguj się.

3.INSTRUKCJA POSTĘPOWANIA NW. UTRATY LUB KRADZIEŻY DANYCH UWIERZYTELNIAJĄCYCH KLIENTA WYKORZYSTYWANYCH DO LOGOWANIA LUB PRZEPROWADZANIA TRANSAKCJI.

3.1. TELEKOD

Jeśli zgubiłeś/aś bądź zapomiałeś/aś Telekod, to skontaktuj się z Infolinią pod numerem 0 801 900 700 lub +48 22 488 55 50. Nowy telekod zostanie wysłany SMS-em po pozytywnej weryfikacji Twoich danych osobowych.

3.2. TOKEN (KLUCZ)

Jeśli zgubisz lub zostanie Ci skradziony Token, to:

a) zgłoś to niezwłocznie dzwoniąc na Infolinię pod numer 0 801 900 700 lub +48 22 488 55 50. Po połączeniu wybierz opcję: (1) – Usługi bankowe, potem (4) – Konta, Lokaty, Karty i Pożyczki i zautoryzuj się używając numeru klienta lub numeru karty i telekodu, a następnie połącz się z Doradcą wybierając(9). UWAGA! Jeśli po połączeniu z Infolinią nie możesz zautoryzować się w automatycznym serwisie telefonicznymi (IVR), pamiętaj, że zgłaszając nam zagubienie lub utratę tokena zostaniesz dodatkowo zweryfikowany przez Doradcę Contact Center prowadzącego rozmowę. Pozytywna weryfikacja spowoduje zablokowanie dostępu do bankowości elektronicznej. Nowy token zostanie wydany tylko na podstawie telefonicznej dyspozycji po uprzednim zautoryzowaniu się w IVR (z użyciem numeru klienta i telekodu) lub dyspozycji pisemnej z podpisem zgodnym ze wzorem posiadanym przez Bank (złożonym podczas zawierania umowy);
b) możesz nam to zgłosić również wysyłając wiadomość na kontakt@toyotabank.pl. W treści zgłoszenia podaj swój numer klienta (identyfikator) i jeśli to możliwe - numer utraconego tokena. Dostęp do bankowości elek-

tronicznej zostanie niezwłocznie zablokowany, a następnie podejmiemy próbę kontaktu w celu potwierdzenia zaistniałego zdarzenia i wydania nowego tokena lub odblokowania dostępu do systemu bankowości elektronicznej;
c) w okresie niedostępności Contact Center masz możliwość automatycznego zastrzeżenia dostępu do bankowości elektronicznej przez Infolinię. W najbliższym możliwym terminie skontaktujemy się z Tobą telefonicznie i po pozytywnej weryfikacji Twoich danych osobowych zablokujemy dostęp.

3.3. APLIKACJA „MOBILNA AUTORYZACJA TOYOTA BANK"

Jeśli zgubisz urządzenie mobilne z zainstalowaną aplikacją, to:

Zgłoś to niezwłocznie na Infolinię pod numer 0 801 900 700 lub +48 22 488 55 50. Po połączeniu wybierz opcję: (1) – Usługi bankowe, potem (4) – Konta, Lokaty, Karty i Pożyczki i zautoryzuj się używając numeru klienta lub numeru karty i telekodu, a następnie połącz się z Doradcą wybierając(9).

UWAGA! Jeśli po połączeniu z Infolinią nie możesz zautoryzować się w automatycznym serwisie telefonicznymi (IVR), pamiętaj, że zgłaszając nam zagubienie lub utratę telefonu (urządzenia mobilnego) z zainstalowaną aplikacją mobilna do autoryzacji, zostaniesz dodatkowo zweryfikowany przez Doradcę Contact Center prowadzącego rozmowę. Pozytywna weryfikacja spowoduje zablokowanie dostępu do bankowości elektronicznej.

Odblokowanie dostępu zostanie zrealizowane tylko na podstawie telefonicznej dyspozycji po uprzednim zautoryzowaniu się w IVR (z użyciem numeru klienta i telekodu) lub dyspozycji pisemnej z podpisem zgodnym ze wzorem posiadanym przez Bank (złożonym podczas zawierania umowy).

UWAGA! W związku z koniecznością zachowania obowiązujących przepisów prawa Twoja tożsamość musi ponownie zostać zweryfikowana. Przed odblokowaniem możliwości dalszego korzystania z aplikacji mobilnej lub jej instalacji na nowym urządzeniu wyślemy do Ciebie kuriera w celu potwierdzenia złożonej dyspozycji i Twoich danych osobowych. O zakończeniu całej procedury zostaniesz poinformowany telefonicznie.

4. PORADNIK

Zapoznaj się z komunikatem Komisji Nadzoru Finansowego, dotyczącym podstawowych zasad bezpieczeństwa w zakresie bankowości elektronicznej i korzystaniu z kart płatniczych.

Zawsze zgłaszaj do banku:
a) podejrzenia przejęcia lub utraty danych do logowania do systemu bankowości internetowej lub Infolinii. Zasady obowiązujące przy zgłaszaniu tego typu zdarzeń zostały opisane w sekcji Instrukcja postępowania nw. utraty lub kradzieży danych uwierzytelniających klienta wykorzystywanych do logowania lub przeprowadzania transakcji;
b) otrzymanie podejrzanej wiadomości e-mail z prośbą o podanie danych osobowych i/lub danych do logowania do bankowości elektronicznej;
c) wszelkie podejrzane i niestandardowe zdarzenia, które uznasz za zagrażające bezpieczeństwu Twoich środków zgromadzonych w Toyota Bank.

Możesz się z nami skontaktować przez Infolinię (801 900 700 lub +48 22 488 55 50) lub bezpieczną pocztę elektroniczną dostępną w Systemie Bankowości Elektronicznej.

Zachęcamy do skorzystania z platformy edukacyjnej Biura Informacji Kredytowej Score Hunter. W serwisie można

zdobyć wiedzę na temat:
a) budowania historii kredytowej;
b) wiarygodności i ochrony tożsamości.

Przygotowano także quizy i pytania, na które odpowiedzi można znaleźć w materiałach video i tekstach poradnikowych. Użytkownicy mogą również zbierać punkty i wymieniać je na nagrody.

Szczegółowe informacje dostępne są na stronie: www.scorehunter.pl