Kurpiowski Bank Spółdzielczy w Myszyńcu

Grupa BPS

Lista zmian:

Zapis przed zmianą	Zapis po zmianie
par 2 pkt 18 „18) **dostawca usług** – dostawca usług określonych w § 2 pkt 82-84, oraz dostawca świadczący wyłącznie usługę określoną w § 2 pkt 82, spełniający wymagania ustawy UUP ;	par 2 pkt 19 „18) **dostawca usług – dostawca usług** – dostawca usług określonych w § 2 pkt 84-86, oraz dostawca świadczący wyłącznie usługę określoną w § 2 pkt 84, spełniający wymagania ustawy UUP ;
par 2 pkt 24 **„24) Hasło 3D Secure** –przesyłane – w postaci wiadomości tekstowej SMS na wskazany przez Użytkownika karty krajowy numer telefonu komórkowego – jednorazowe hasło służące do identyfikacji Użytkownika karty i uwierzytelnienia jego dyspozycji w ramach potwierdzenia transakcji internetowych z wykorzystaniem zabezpieczenia 3D Secure.”	par 2 pkt 25 **„24) Uwierzytelnieni 3D Secure** –przesyłane – w postaci wiadomości tekstowej SMS na wskazany przez Użytkownika karty krajowy numer telefonu komórkowego – jednorazowe hasło służące do identyfikacji Użytkownika karty i uwierzytelnienia jego dyspozycji w ramach potwierdzenia transakcji internetowych z wykorzystaniem zabezpieczenia 3D Secure lub metoda autoryzacji w aplikacji Mobilnej o ile Bank udostępnia taką funkcjonalność.”
par 2 pkt 35 **„35) limity transakcyjne** – kwota, do wysokości której Posiadacz rachunku/Użytkownik karty może dokonywać transakcji gotówkowych lub bezgotówkowych w ciągu jednego dnia. Wysokość limitu ustalona jest indywidualnie dla każdej z wydanych kart oraz wymienionych transakcji	Par 2 pkt 35 „35) **limity transakcyjne** - kwota, do wysokości której Posiadacz rachunku/Użytkownik karty może dokonywać transakcji gotówkowych lub bezgotówkowych z uwzględnieniem faktu, że limit transakcji internetowych zawiera się w limicie transakcji bezgotówkowych. Wysokość limitu ustalona jest indywidualnie dla każdej z wydanych kart oraz wymienionych transakcji, a w przypadku braku ustalenia limitów indywidualnych zastosowanie znajdują domyślne limity transakcyjne, które są określane przez Bank i udostępniane przez Bank na swojej stronie internetowej, w Oddziale”
par 2 pkt 69 **„69) silne uwierzytelnienie** - uwierzytelnianie zapewniające ochronę poufności danych w oparciu o zastosowanie co najmniej dwóch elementów należących do kategorii: **a)** wiedza o czymś, o czym wie wyłącznie Użytkownik/ Użytkownik karty,	Par 2 pkt 69 **„69) silne uwierzytelnienie** - uwierzytelnianie zapewniające ochronę poufności danych w oparciu o zastosowanie co najmniej dwóch elementów należących do kategorii: **a)** wiedza o czymś, o czym wie wyłącznie Użytkownik/ Użytkownik karty,

b) posiadanie czegoś, co posiada wyłącznie Użytkownik/ Użytkownik karty, **c)** cechy charakterystyczne Użytkownika/ Użytkownika karty, będących integralną częścią tego uwierzytelniania oraz niezależnych w taki sposób, że naruszenie jednego z tych elementów nie osłabia wiarygodności pozostałych;	**b)** posiadanie czegoś, co posiada wyłącznie Użytkownik/ Użytkownik karty, **c)** cechy charakterystyczne Użytkownika/ Użytkownika karty, będących integralną częścią tego uwierzytelniania oraz niezależnych w taki sposób, że naruszenie jednego z tych elementów nie osłabia wiarygodności pozostałych; Zgodnie z ustawą o usługach płatniczych Bank może nie stosować silnego uwierzytelnienia w przypadku transakcji internetowej jeżeli zostały spełnione następujące warunki: (1) kwota transakcji internetowej nie przekracza kwoty opublikowanej na stronie Banku www.kbsmyszyniec.pl oraz (2) łączna kwota poprzednich transakcji internetowych zainicjowanych przez płatnika od dnia ostatniego zastosowanego silnego uwierzytelnienia nie przekracza kwoty opublikowanej na stronie Banku www.kbsmyszyniec.pl, lub (3) liczba poprzednio wykonanych transakcji internetowych zainicjowanych przez płatnika nie przekracza pięciu następujących po sobie pojedynczych transakcji internetowych;”
par 2 pkt 72 – 73 **„72) system bankowości elektronicznej** – system umożliwiający samoobsługowy dostęp do rachunków bankowych Posiadacza rachunku oraz dostęp do innych produktów bankowych za pomocą sieci Internet i przeglądarki internetowej; **73)system bankowości mobilnej** – system umożliwiający samoobsługowy dostęp do rachunków bankowych Posiadacza rachunku oraz dostęp do innych produktów bankowych;”	**par 2 pkt 72 - 73** **„72) system bankowości elektronicznej** – system umożliwiający samoobsługowy dostęp do rachunków bankowych Posiadacza rachunku oraz dostęp do innych produktów bankowych za pomocą systemu bankowości internetowej oraz systemu bankowości mobilnej; **73) system bankowości mobilnej** – system umożliwiający samoobsługowy dostęp do rachunków bankowych Posiadacza rachunku oraz dostęp do innych produktów bankowych za pomocą dedykowanej aplikacji mobilnej. Aplikacja do pobrania ze sklepów internetowych w zależności od posiadanego urządzenia mobilnego;”
par 2 pkt 74 - brak	**par 2 pkt 74** **„74) system bankowości internetowej** - integralna część systemu bankowości elektronicznej umożliwiająca dostęp do rachunków i produktów bankowych za pomocą przeglądarki internetowej. Logowanie do systemu dostępne jest z poziomu strony internetowej Banku znajdującej się pod adresem WWW.kbsmyszyniec.pl”

par 35 ust 7 - brak	par 35 ust 7 „7. Bank nie realizuje przelewów otrzymanych w walucie PLN na rachunki walutowe Posiadacza rachunku za pośrednictwem systemów Elixir, Express Elixir i SORBNET.”
par 67 „Użytkownik karty jest zobowiązany do podpisania karty podpisem zgodnym ze wzorem podpisu obowiązującym w Banku.	par 67 „Jeśli karta posiada wyznaczone do tego miejsce, Użytkownik karty jest zobowiązany do podpisania karty podpisem zgodnym ze wzorem podpisu obowiązującym w Banku.”
par 68 ust 4 pkt 1 „1) podpisania karty zgodnie ze wzorem podpisu złożonym na wniosku;”	par 68 ust 8 pkt 1 „1) podpisania karty zgodnie ze wzorem podpisu złożonym na wniosku jeśli posiada ona wyznaczone do tego miejsce”
par 58 ust 5 pkt 1 „1) podpisania karty;”	par 58 ust 5 pkt 1 „1) podpisania karty jeśli posiada ona wyznaczone do tego miejsce”
par 76 ust 3 „Hasło 3D Secure jest unikalne dla każdej transakcji internetowej, dla której zostanie wygenerowane. Trzykrotne błędne wprowadzenie Hasła 3D Secure spowoduje zablokowanie wykonania transakcji internetowej. Posiadacz rachunku/Użytkownik karty może odblokować wykonywanie transakcji internetowych tego samego dnia za pośrednictwem Infolinii Banku bądź w placówce Banku. W przeciwnym wypadku wykonywanie transakcji internetowych zostanie automatycznie odblokowane następnego dnia”	par 76 ust 3 „Uwierzytelnienie 3D Secure przesłane – w postaci wiadomości tekstowej SMS - jest unikalne dla każdej transakcji internetowej, dla której zostanie wygenerowane. Trzykrotne błędne wprowadzenie Hasła 3D Secure spowoduje zablokowanie wykonania transakcji internetowej z zabezpieczeniem 3D Secure. Posiadacz rachunku/Użytkownik karty może odblokować zabezpieczenie 3D Secure tego samego dnia za w placówce Banku. W przeciwnym wypadku zabezpieczenie 3D Secure zostanie automatycznie odblokowane następnego dnia.”
par 80 ust 1 pkt 4) „limitu jednorazowej wypłaty gotówki w ramach usługi cash back wynoszącego 300 PLN (karty VISA); warunkiem wypłaty jest jednoczesne dokonanie transakcji bezgotówkowej dokonanej na terenie Polski, z wyłączeniem karty wydanej w walucie rozliczeniowej innej niż PLN – nie jest możliwa sama wypłata gotówki”	par 80 ust 1 pkt 4) „limitu jednorazowej wypłaty gotówki w ramach usługi cash back wynoszącego 1000 PLN; warunkiem wypłaty jest jednoczesne dokonanie transakcji bezgotówkowej dokonanej na terenie Polski, z wyłączeniem karty wydanej w walucie rozliczeniowej innej niż PLN – nie jest możliwa sama wypłata gotówki”
par 80 ust 3	par 80 ust 3

„2. Posiadacz rachunku może zdefiniować dla karty własne dzienne limity transakcyjne, niższe od limitów transakcyjnych określonych przez Bank w ust. 1 pkt. 1 i 2, i może je w każdej chwili zmieniać poprzez system bankowości elektronicznej, portal kartowy oraz poprzez złożenie odrębnej dyspozycji w Banku, jak również wyzerować wybrane limity transakcyjne, jeśli nie będzie korzystał z danego typu transakcji lub ze względów bezpieczeństwa.”	„3. Posiadacz rachunku/Użytkownik karty może zdefiniować dla karty własne limity transakcyjne dla transakcji bezgotówkowych, w tym internetowych, jak i gotówkowych, niższe od limitów transakcyjnych określonych przez Bank w ust. 1 pkt 1 i 2, i może je w każdej chwili zmieniać poprzez system bankowości elektronicznej, portal kartowy oraz poprzez złożenie odrębnej dyspozycji w Banku, jak również wyzerować wybrane limity transakcyjne, jeśli nie będzie korzystał z danego typu transakcji lub ze względów bezpieczeństwa.”
par 87 „1. W celu korzystania z usługi bankowości elektronicznej Bank wydaje Użytkownikom następujące środki dostępu: 1) identyfikator Użytkownika; 2) hasło aktywacyjne w formie elektronicznej lub w postaci wydruku umożliwiające aktywację dostępu do systemu. 2. Korzystanie z systemu bankowości mobilnej po pierwszym zalogowaniu wymaga używania kodu e-PIN, ustanowionego przez Użytkownika w systemie bankowości mobilnej. 3. Środki dostępu mogą stanowić uwierzytelnienie lub element silnego uwierzytelnienia Użytkownika oraz element autoryzacji transakcji płatniczych i innych dyspozycji w systemie bankowości elektronicznej. 4. Od dnia 05 maja 2019 r. Bank nie stosuje haseł jednorazowych”	par 87 „1. W celu korzystania z usługi bankowości elektronicznej Bank wydaje Użytkownikom login będący identyfikatorem Użytkownika, niezbędnym w procesie logowania. 2. Podczas uruchomienia usługi bankowości elektronicznej Klient otrzymuje hasło tymczasowe do pierwszego logowania do systemu bankowości internetowej w formie wiadomości SMS lub wydruku wygenerowanego przez pracownika Banku, umożliwiające ustawienie własnego hasła stałego, wykorzystywanego w każdym kolejnym procesie logowania. 3. Korzystanie z systemu bankowości mobilnej przy pierwszym zalogowaniu wymaga ustawienia własnego kodu e-PIN. 4. Środki dostępu mogą stanowić uwierzytelnienie lub element silnego uwierzytelnienia Użytkownika oraz element autoryzacji transakcji płatniczych i innych dyspozycji w systemie bankowości elektronicznej. 5. . Od dnia 05 maja 2019 r. Bank nie stosuje haseł jednorazowych”
par 90 ust 2 „2. Po 90 dniach od ostatniej poprawnej zmiany hasła oraz e-PINu, Użytkownik zobowiązany jest do zmiany obecnie używanego hasła do logowania/ e-PINu lub do uwierzytelnienia obecnie używanego hasła/ e-PINu. Każde z podjętych przez Użytkownika działań wymaga autoryzacji zgodnie z metodami opisanymi w §89 od dnia wejścia w życie niniejszego ustępu lub od pierwszego	par 90 ust 2 „2. Po 90 dniach od ostatniej poprawnej zmiany hasła oraz e-PINu, Użytkownik zobowiązany jest do zmiany obecnie używanego hasła do logowania/ e-PINu lub do uwierzytelnienia obecnie używanego hasła/ e-PINu.

skorzystania z usługi bankowości elektronicznej po tym dniu.”	Każde z podjętych przez Użytkownika działań wymaga autoryzacji zgodnie z metodami opisanymi w §89.”
par 91 „1. W przypadku utraty, kradzieży, wejścia w posiadanie lub podejrzenia wejścia w posiadanie środków dostępu do systemu bankowości elektronicznej przez osobę nieuprawnioną Użytkownik składa dyspozycję zablokowania dostępu do systemu bankowości elektronicznej. W imieniu osoby małoletniej dyspozycję składa przedstawiciel ustawowy. 2. Dyspozycja może być złożona pisemnie w placówce Banku. 3. Pracownik Banku potwierdza Użytkownikowi przyjęcie dyspozycji zablokowania, podając identyfikator zgłoszenia lub datę, godzinę, imię i nazwisko pracownika przyjmującego dyspozycję (w przypadku dyspozycji telefonicznych) lub wydając kopię dyspozycji (w przypadku dyspozycji pisemnej). 4. Dyspozycja zablokowania wykonywana jest przez pracownika Banku niezwłocznie po otrzymaniu dyspozycji od Użytkownika. 5. Dyspozycję zablokowania, o której mowa w ust. 1, każdy Użytkownik składa w odniesieniu do własnego dostępu	par 91 „1. W przypadku utraty, kradzieży, wejścia w posiadanie lub podejrzenia wejścia w posiadanie środków dostępu do systemu bankowości elektronicznej przez osobę nieuprawnioną Użytkownik składa dyspozycję zablokowania dostępu do systemu bankowości elektronicznej. W imieniu osoby małoletniej dyspozycję składa przedstawiciel ustawowy. 2. Dyspozycja może być złożona pisemnie w placówce Banku lub w systemie bankowości elektronicznej. 3. Pracownik Banku potwierdza Użytkownikowi przyjęcie dyspozycji zablokowania, wydając kopię dyspozycji (w przypadku dyspozycji pisemnej). 4. Dyspozycja zablokowania wykonywana jest przez pracownika Banku niezwłocznie po otrzymaniu dyspozycji od Użytkownika. 5. W przypadku złożenia dyspozycji blokady za pomocą systemu bankowości elektronicznej, dyspozycja ta realizowana jest automatycznie, bez udziału pracownika Banku. 6. Dyspozycję zablokowania, o której mowa w ust. 1, każdy Użytkownik składa w odniesieniu do własnego dostępu”

W związku z opisanymi wyżej zmianami, odpowiednim zmianom ulega również dotychczasowa numeracja jednostek redakcyjnych, odesłań lub przypisów w ww. dokumencie.

Zarząd
Kurpiowskiego Banku Spółdzielczego
w Myszyńcu