Zasady udostępniania i funkcjonowania elektronicznych kanałów dostępu

Rozdział 1 Udostępnienie i warunki korzystania z usług bankowości elektronicznej

§ 1

1. Bank może świadczyć użytkownikom usługi w zakresie obsługi produktów i usług za pośrednictwem następujących elektronicznych kanałów dostępu:
   1) w ramach bankowości elektronicznej:
      a) bankowość internetowa (serwis internetowy - Internet Banking) – dostęp i dyspozycje składane na komputerze lub urządzeniu mobilnym przy użyciu przeglądarki internetowej;
      b) bankowość mobilna – dostęp i dyspozycje składane przy użyciu zaufanego urządzenia mobilnego, za pomocą aplikacji mobilnej SGB Mobile[1];
   2) powiadomień SMS (serwis SMS) – uzyskiwanie informacji związanych z transakcjami na rachunku w formie wiadomości SMS;
2. Serwis internetowy, o którym mowa w ust. 1 pkt 1 ppkt a, jest dostępny w dwóch wariantach:
   1) wariant I - z jednoosobową autoryzacją dyspozycji;
   2) wariant II - z jedno lub wieloosobową autoryzacją dyspozycji, przy czym wieloosobowa autoryzacja możliwa jest dla usługi Internet Banking (@Firma),

   z zastosowaniem wymaganych przez bank metod uwierzytelniania.
3. Wykaz produktów i usług dostępnych za pośrednictwem bankowości elektronicznej oraz warunki korzystania z usług określa przewodnik użytkownika publikowany na stronie internetowej banku; przewodnik użytkownika stanowi instrukcję użytkowania zawierającą opis poszczególnych elektronicznych kanałów dostępu, wymagania techniczne dla każdego kanału i zasady prawidłowego posługiwania się tymi kanałami przez klienta.
4. Zakres funkcjonalny serwisu internetowego, o którym mowa w ust. 1 pkt 1 ppkt a, jest opisany w przewodniku użytkownika.
5. Bank udostępnia klientowi usługę bankowości mobilnej w przypadku posiadania, w ramach zawartej umowy, dostępu do usługi bankowości internetowej[2].
6. Informacje dotyczące aktualnej oferty usług dostępnych w aplikacji mobilnej SGB Mobile oraz zasady jej udostępniania opisane są w Regulaminie korzystania z aplikacji mobilnej SGB Mobile, zamieszczonym na stronie internetowej banku.
7. W serwisie internetowym użytkownicy mogą mieć dostęp i autoryzować operacje jedno lub wieloosobowo, zgodnie z kartą wzorów podpisów posiadacza rachunku, z zastosowaniem wymaganych przez bank metod uwierzytelniania.

§ 2

1. Bankowość elektroniczna dostępna jest dla klientów posiadających w banku rachunek bieżący prowadzony w złotych, chyba że Regulamin korzystania z aplikacji mobilnej SGB Mobile stanowi inaczej.
2. Posiadacz rachunku może wnioskować o udostępnienie kolejnych produktów lub usług oraz zmianę warunków świadczenia tych produktów lub usług i zawierać umowy za pośrednictwem elektronicznych kanałów dostępu, o ile taki sposób został udostępniony przez bank; szczegółowe zasady składania oświadczeń woli przez użytkownika oraz bank dotyczące zawarcia umowy lub zmiany jej warunków za pośrednictwem elektronicznych kanałów dostępu określone są § 7; informacje o ofercie oraz dostępnych sposobach zawierania umów znajdują się na stronie internetowej banku oraz w przewodniku użytkownika.

§ 3

1. Użytkownik uzyskuje dostęp do bankowości elektronicznej za pomocą indywidualnych danych uwierzytelniających, z zastrzeżeniem § 9.
2. Bank może umożliwić korzystanie z usługi przy użyciu tych samych indywidualnych danych uwierzytelniających użytkownikowi będącemu równocześnie posiadaczem/ pełnomocnikiem do innego rachunku, z uwzględnieniem limitów operacji[3], o których mowa w rozdziale 7 niniejszego załącznika.

§ 4

1. W przypadku dokonywania transakcji z wykorzystaniem bankowości elektronicznej:
   1) zaleca się korzystanie z zaufanych komputerów posiadających aktualne oprogramowanie antywirusowe;

[1] po wdrożeniu usługi przez bank
[2] po udostępnieniu usługi przez bank, o czym bank poinformuje na swojej stronie internetowej
[3] standardowy limit może zostać samodzielnie zmieniony w systemie transakcyjnym przez posiadacza rachunku po zatwierdzeniu zmienionej kwoty limitu kodem autoryzacyjnym

2) należy sprawdzić czy transmisja jest szyfrowana protokołem SSL (ang. Secure Socket Layer), który zapewnia poufność i integralność transmisji danych;
3) nie należy korzystać z otwartych i niezabezpieczonych sieci.

2. Użytkownikiem niebędącym posiadaczem rachunku może być wyłącznie osoba, której posiadacz rachunku udzielił pełnomocnictwa stałego, chyba że z treści umowy wynika inaczej; użytkownikiem może być również inna osoba wskazana przez posiadacza rachunku, niebędąca pełnomocnikiem stałym, którą posiadacz rachunku wskazał jako pasywnego użytkownika.
3. Warunkiem korzystania z usługi jest obsługa plików *cookies* w przeglądarce internetowej, które są konieczne do utrzymania aktywnej sesji po zalogowaniu się do bankowości internetowej; szczegółowe informacje dotyczące rodzaju stosowanych plików *cookies* oraz celu ich wykorzystywania dostępne są na stronie internetowej banku.

§ 5

1. Użytkownik/pasywny użytkownik ma obowiązek korzystać z elektronicznych kanałów dostępu zgodnie z umową i regulaminem i przewodnikiem użytkownika oraz zabezpieczyć otrzymane indywidualne dane uwierzytelniające przed dostępem osób nieuprawnionych i zapewnia ich poufność.
2. Użytkownik/pasywny użytkownik uzyskuje dostęp do rachunku poprzez udostępnione mu indywidualne dane uwierzytelniające.
3. Z chwilą otrzymania indywidualnych danych uwierzytelniających, użytkownik/pasywny użytkownik podejmuje niezbędne środki służące zapobieżeniu naruszenia indywidualnych danych uwierzytelniających, w szczególności przyjmuje do wiadomości, że ze względów bezpieczeństwa poszczególnych indywidualnych danych uwierzytelniających nie wolno przetrzymywać razem ze sobą.
4. Bank zapewnia należytą ochronę indywidualnych danych uwierzytelniających; indywidualne dane uwierzytelniające są dostępne wyłącznie dla użytkownika/pasywnego użytkownika uprawnionego do korzystania z nich.

§ 6

Zmiana zakresu usług przez bank, wymaga zachowania warunków i trybu przewidzianego dla zmiany regulaminu.

Rozdział 2 Dyspozycje składane za pośrednictwem elektronicznych kanałów dostępu

§ 7

1. Wszelkie oświadczenia woli, w tym dotyczące zawarcia umowy i zmiany jej warunków, składane wobec banku przez użytkownika w postaci elektronicznej będą ważne i wiążące pod względem prawnym dla posiadacza rachunku i banku, jeżeli przy użyciu indywidualnych danych uwierzytelniających dokonana została poprawna identyfikacja użytkownika składającego oświadczenie woli, z zastosowaniem wymaganych przez bank metod uwierzytelniania, przy uwzględnieniu wymogów silnego uwierzytelniania.
2. Użytkownik składa oświadczenie woli zawarcia umowy w postaci elektronicznej, zrównanej z formą pisemną zgodnie z art. 7 ustawy Prawo bankowe, z wykorzystaniem indywidualnych danych uwierzytelniających.
3. Bank składa oświadczenie woli zawarcia umowy w postaci elektronicznej, zrównanej z formą pisemną zgodnie z art. 7 ustawy Prawo bankowe, opatrując dokument umowy pieczęcią elektroniczną.
4. Bank może zawierać umowy z użytkownikiem za pośrednictwem elektronicznych kanałów dostępu posługując się pełnomocnikiem. Pełnomocnik składa w imieniu banku oświadczenie woli zawarcia umowy w postaci elektronicznej, zrównanej z formą pisemną zgodnie z art. 7 ustawy Prawo bankowe, zgodnie z zasadami określonymi w ust. 3.
5. Umowa zawierana jest w postaci elektronicznej z chwilą opatrzenia dokumentu umowy pieczęcią elektroniczną. Umowę podpisaną w sposób, o którym mowa w ust. 3 i 4, bank udostępnia użytkownikowi w sposób określony w umowie.
6. Użytkownik ma prawo odstąpić od umowy zawartej za pośrednictwem elektronicznych kanałów dostępu bez podania przyczyny w terminie i na warunkach określonych w umowie.

§ 8

1. Do dysponowania rachunkami za pośrednictwem elektronicznych kanałów dostępu mają zastosowanie ogólne zasady dotyczące dysponowania rachunkami określone w rozdziale 2 regulaminu, dotyczące poszczególnych rodzajów rachunków, z zastrzeżeniem postanowień § 9-13 niniejszego załącznika oraz sposobu posługiwania się elektronicznym kanałem dostępu opisanym w przewodniku użytkownika.

2. Bank świadczy usługę oferowaną przez integratorów płatności internetowych, którzy inicjują płatności w formie przelewów typu pay by link przy czym:
   1) integratorem płatności internetowych jest podmiot świadczący usługi sklepom internetowym lub innym podmiotom prowadzącym sprzedaż towarów lub usług, polegające na udostępnieniu im możliwości przyjmowania płatności od ich klientów za pomocą przelewów typu pay by link,
   2) przelew typu pay by link jest realizowany przez klienta dokonującego zapłaty za zakupy w sklepach internetowych lub u innych podmiotów prowadzących sprzedaż towarów lub usług za pośrednictwem integratorów płatności internetowych.
3. Zgody na wykonanie transakcji płatniczej użytkownik może udzielić również za pośrednictwem dostawcy świadczącego usługę inicjowania transakcji płatniczej.
4. W przypadku inicjowania transakcji przez dostawcę świadczącego usługę inicjowania transakcji lub przez odbiorcę lub za jego pośrednictwem, posiadacz rachunku nie może odwołać zlecenia płatniczego po udzieleniu dostawcy świadczącemu usługę inicjowania transakcji zgody na zainicjowanie transakcji albo po udzieleniu odbiorcy zgody na wykonanie transakcji.
5. Pasywny użytkownik systemu nie może autoryzować dyspozycji.
6. Bank umożliwia w serwisie internetowym:
   1) składanie innych wniosków udostępnionych przez bank oraz zawieranie umów na zasadach określonych w § 7;
   2) składanie innych wniosków udostępnionych przez bank dotyczących produktów lub usług podmiotów trzecich współpracujących z bankiem.

   Bank może udostępnić w serwisie internetowym inne wnioski.

§ 9

1. Wszelkie dyspozycje i zlecenia płatnicze w bankowości elektronicznej, użytkownik składa bankowi w formie elektronicznej, po jego uwierzytelnieniu, w sposób umożliwiający bankowi identyfikację użytkownika i zapoznanie się z treścią dyspozycji; wyżej wymienione dyspozycje spełniają wymagania formy pisemnej w zakresie, w jakim mają związek z czynnościami bankowymi (zgodnie z art. 7 ustawy Prawo bankowe).
2. Po złożeniu dyspozycji lub zlecenia płatniczego w bankowości elektronicznej, użytkownik dokonuje ich autoryzacji przy użyciu indywidualnych danych uwierzytelniających z zastosowaniem wymaganych przez bank metod uwierzytelniania, z zastrzeżeniem ust. 3.
3. Bank stosuje silne uwierzytelnianie, w przypadku gdy użytkownik/pasywny użytkownik:
   1) uzyskuje dostęp do swojego rachunku w trybie online;
   2) inicjuje transakcję płatniczą;
   3) przeprowadza za pomocą kanału zdalnego czynność, która może wiązać się z ryzykiem oszustwa związanego z wykonywanymi usługami płatniczymi lub innych nadużyć,

   za wyjątkiem sytuacji nie wymagających silnego uwierzytelniania wskazanych w ust 4.
4. Bank może nie stosować silnego uwierzytelniania w następujących przypadkach:
   1) dostępu użytkownika/pasywnego użytkownika do jednej z wymienionych niżej pozycji w trybie online lub do obu tych pozycji bez ujawniania szczególnie chronionych danych dotyczących płatności:
      a) salda rachunku,
      b) transakcji płatniczych przeprowadzonych w ciągu ostatnich 90 dni za pośrednictwem rachunku, z zastrzeżeniem ust. 5;
   2) inicjowania transakcji, której odbiorca znajduje się na liście zaufanych odbiorców utworzonej uprzednio przez użytkownika;
   3) inicjowania kolejnych transakcji należących do serii transakcji cyklicznych, opiewających na tę samą kwotę na rzecz tego samego odbiorcy pod warunkiem, że utworzenie, zmiana lub zainicjowanie pierwszej transakcji cyklicznej odbyło się przy zastosowaniu silnego uwierzytelnienia;
   4) jeżeli użytkownik inicjuje transakcję płatniczą w sytuacji, gdy płatnik i odbiorca są tą samą osobą fizyczną lub prawną i oba rachunki płatnicze są prowadzone przez bank;
   5) inicjowania zdalnej transakcji, którą bank uzna za charakteryzującą się niskim poziomem ryzyka zgodnie z mechanizmami monitorowania transakcji.
5. Bank stosuje silne uwierzytelnianie użytkownika, jeżeli spełniony jest którykolwiek z następujących warunków:
   1) użytkownik/pasywny użytkownik uzyskuje dostęp do informacji określonych w ust. 4 pkt 1 lit. a, w trybie online po raz pierwszy;

2) minęło więcej niż 90 dni odkąd użytkownik ostatni raz uzyskał dostęp do informacji określonych w ust. 4 pkt 1 lit. b w trybie online oraz odkąd ostatni raz zastosowano silne uwierzytelnianie użytkownika/pasywnego użytkownika.

6. Bank zastrzega sobie prawo kontaktu z użytkownikiem w celu realizacji zlecenia płatniczego.
7. Dostęp użytkownika/pasywnego użytkownika do serwisu internetowego następuje poprzez podanie identyfikatora użytkownika i hasła.
8. Autoryzacja dyspozycji składanych za pośrednictwem serwisu internetowego odbywa się poprzez użycie następujących indywidualnych danych uwierzytelniających:
   1) nPodpis – certyfikat plus Aplikacja kryptograficzna[4] lub
   2) hasło SMS lub
   3) aplikacji mobilnej.
9. Jeżeli użytkownik, podczas procesu logowania się do bankowości internetowej doda urządzenie, z którego loguje się do bankowości internetowej jako urządzenie zaufane, kolejne logowania z tego urządzenia do bankowości internetowej w przeglądarce nie będą wymagały dodatkowego uwierzytelnienia użytkownika za pomocą wybranej metody autoryzacyjnej[5]. Urządzeniem zaufanym może być np. prywatny komputer, smartfon lub tablet z którego korzysta wyłącznie użytkownik. Bank podczas procesu logowania weryfikuje określone cechy tego urządzenia.
10. Użytkownik w dowolnym momencie ma możliwość poprzez bankowość internetową usunięcia swojego urządzenia zaufanego, a każde kolejne logowanie do bankowości internetowej będzie wymagało dodatkowego potwierdzania, o którym mowa w ust. 9.
11. Autoryzacja dokonana przez użytkownika jest równoznaczna z poleceniem bankowi dokonania określonej czynności i stanowi podstawę jej dokonania.
12. Bank przesyła kody autoryzacyjne wykorzystywane przy stosowanych metodach uwierzytelniania na numer telefonu komórkowego, który użytkownik wskazał w umowie, we wniosku o otwarcie rachunku lub druku pełnomocnictwa.
13. Bank może wprowadzić, wycofać oraz zmienić rodzaj stosowanych indywidualnych danych uwierzytelniających poprzez udostępnienie ich użytkownikowi/pasywnemu użytkownikowi oraz zawiadomienie go o dokonanej zmianie; informacja o stosowanych indywidualnych danych uwierzytelniających jest zamieszczona w przewodniku użytkownika oraz na stronie internetowej banku.

§ 10

Jeżeli z postanowień umowy, regulaminu lub obowiązujących przepisów prawa nie wynika nic innego, chwilą złożenia przez użytkownika oświadczenia w postaci elektronicznej, w szczególności złożenia dyspozycji lub dokonania jakiejkolwiek czynności faktycznej, jest moment zarejestrowania odpowiednich danych w bankowości elektronicznej i przyjęcia tego oświadczenia przez serwer banku.

§ 11

1. Realizacja dyspozycji składanych za pośrednictwem bankowości elektronicznej odbywa się elektronicznie, przy czym użytkownik zobowiązuje się do stosowania zasad autoryzacji wymaganych dla bankowości internetowej.
2. Autoryzowane zlecenie płatnicze nie może zostać odwołane, za wyjątkiem sytuacji określonych w § 24 ust. 6-9 regulaminu.

§ 12

1. Przyjęcie do realizacji dyspozycji złożonej za pośrednictwem elektronicznych kanałów dostępu bank potwierdza w formie informacji wysyłanej za pośrednictwem tego kanału.
2. W przypadku nieprzyjęcia przez bank dyspozycji złożonej za pośrednictwem elektronicznych kanałów dostępu z powodu:
   1) jej niekompletności;
   2) złożenia dyspozycji sprzecznych ze sobą;
   3) podania nieprawidłowego numeru rachunku odbiorcy;
   4) przekroczenia limitu pojedynczej operacji lub limitu wszystkich operacji w ciągu dnia;
   5) braku środków pieniężnych dla realizacji dyspozycji lub
   6) innych okoliczności uniemożliwiających jej przyjęcie przez bank,

   użytkownik otrzyma za pośrednictwem bankowości elektronicznej informację o fakcie i przyczynie niezrealizowania dyspozycji za pośrednictwem elektronicznego kanału dostępu lub od pracownika placówki banku.

§ 13

[4] dotyczy usługi Internet Banking (@Firma)

[5] po wprowadzeniu funkcjonalności przez bank. W przypadku wdrożenia ww. funkcjonalności informacja zostanie zamieszczona na stronach internetowych banku i przewodniku użytkownika.

1. Bank ma prawo odmowy wykonania dyspozycji złożonej i uwierzytelnionej w bankowości elektronicznej w przypadku gdy:
   1) zaistniałe okoliczności uzasadniają wątpliwości, co do:
      a) złożenia lub autoryzacji dyspozycji przez użytkownika,
      b) zgodności dyspozycji z obowiązującymi przepisami prawa;
   2) kwota lub kwoty dyspozycji oraz należne bankowi prowizje i opłaty przekraczają dostępne środki.
2. Bank ma prawo odmowy wykonania lub wprowadzenia dodatkowych ograniczeń i zabezpieczeń w stosunku do dyspozycji składanych za pośrednictwem elektronicznego kanału dostępu, w przypadku wystąpienia ważnych okoliczności uniemożliwiających wykonanie tych dyspozycji, względów bezpieczeństwa lub sprzeczności treści dyspozycji z wiążącymi użytkownika postanowieniami umów zawartych z bankiem.

Rozdział 3 Korzystanie z usług bankowości elektronicznej

§ 14

Za pośrednictwem elektronicznych kanałów dostępu użytkownik/pasywny użytkownik uzyskuje dostęp do wszystkich rachunków otwartych przed dniem aktywowania usługi oraz do rachunków otwartych w terminie późniejszym, chyba że posiadacz rachunku zawnioskował o ograniczony dostęp do rachunku za pośrednictwem elektronicznych kanałów dostępu.

Rozdział 4 Ograniczenia w korzystaniu z usług bankowości elektronicznej

§ 15

1. Bank jest zobowiązany zablokować dostęp do bankowości elektronicznej w jednym z następujących przypadków:
   1) złożenia przez użytkownika dyspozycji zablokowania dostępu do serwisu internetowego;
   2) kolejnego trzykrotnego wpisania nieprawidłowego PIN lub hasła;
   3) zalogowania się do bankowości elektronicznej z innego kraju przed upływem określonego czasu od ostatniego logowania z poprzedniego kraju (blokada lokalizacyjna/geograficzna);
   4) zalogowania się do bankowości elektronicznej z innego adresu IP niż adres wskazany bankowi przez użytkownika systemu do łączenia się z bankiem (ograniczenie geograficzne).
2. Bank ma prawo częściowo ograniczyć lub zablokować dostęp do bankowości elektronicznej i/lub czasowo zablokować wykonanie dyspozycji w następujących przypadkach:
   1) uzasadnionych przyczyn związanych z bezpieczeństwem dostępu do serwisu internetowego i indywidualnych danych uwierzytelniających, w tym w przypadku podejrzenia popełnienia przestępstwa na szkodę użytkownika;
   2) umyślnego doprowadzenia do nieautoryzowanej transakcji płatniczej przez użytkownika lub uzasadnionego podejrzenia, że użytkownik będzie posługiwał się dostępem w sposób niezgodny z regulaminem;
   3) korzystania przez użytkownika z bankowości internetowej niezgodnie z zasadami bezpieczeństwa określonymi w niniejszym załączniku lub w sposób zagrażający bezpieczeństwu korzystania z bankowości internetowej;
   4) dokonywania czynności konserwacyjnych bankowości elektronicznej lub innych systemów teleinformatycznych związanych z wykonaniem umowy, o czym bank z wyprzedzeniem poinformuje na stronie internetowej banku;
   5) dokonywania czynności mających na celu usunięcie awarii, usterek lub nieprawidłowości działania bankowości elektronicznej lub innych systemów teleinformatycznych, związanych z wykonaniem umowy;
   6) wymiany stosowanych indywidualnych danych uwierzytelniających, o czym bank z wyprzedzeniem poinformuje użytkowników w sposób określony w umowie oraz na stronie internetowej banku;
   7) uzasadnionego podejrzenia, iż transakcje na rachunku klienta mają związek z popełnieniem przestępstwa związanego z praniem pieniędzy lub finansowaniem terroryzmu;
   8) gdy na rachunku klienta wystąpi zamrożenie wartości majątkowych;
   9) braku możliwości zastosowania środków bezpieczeństwa finansowego.
3. Bank może uchylić ograniczenie albo blokadę dostępu do bankowości elektronicznej w przypadku, o którym mowa w ust. 2 pkt 1) na wniosek złożony przez posiadacza rachunku, w sposób określony w ust. 4. W takim przypadku bank wydaje użytkownikowi/pasywnemu użytkownikowi nowe indywidualne dane uwierzytelniające lub dokona uchylenia ograniczenia lub blokady przy zachowaniu dotychczasowych danych uwierzytelniających.
4. W przypadku, o których mowa w ust. 2 pkt 1) uchylenie:

1) ograniczenia lub blokady dostępu do bankowości elektronicznej następuje na podstawie telefonicznej lub złożonej w siedzibie lub dowolnej placówce banku dyspozycji klienta;
2) czasowej blokady dyspozycji następuje po telefonicznym lub pisemnym kontakcie pracownika banku z klientem i po potwierdzeniu przez klienta złożonej dyspozycji.

5. Z zastrzeżeniem ust. 6, bank informuje użytkownika o zamiarze zablokowania indywidualnych danych uwierzytelniających w przypadkach określonych w ust. 2 pkt 1) i 3), przed ich zablokowaniem, a jeżeli nie jest to możliwe – niezwłocznie po zablokowaniu telefonicznie.
6. Bank nie przekazuje informacji o zablokowaniu, jeżeli przekazanie tej informacji byłoby nieuzasadnione ze względów bezpieczeństwa lub zabronione na mocy odrębnych przepisów.
7. W przypadkach, o których mowa w ust. 2 pkt 4) i 5) ograniczenie lub blokada dostępu do serwisu internetowego i/lub czasowa blokada dyspozycji następuje przez możliwie krótki okres niezbędny do usunięcia przyczyny ograniczenia lub blokady.

Rozdział 5 Blokowanie i zastrzeganie dostępu do serwisu internetowego

§ 16

1. Dostęp do serwisu internetowego oraz możliwość posługiwania się indywidualnymi danymi uwierzytelniającymi może zostać zablokowany przez:
   1) bank, zgodnie z postanowieniami § 18;
   2) użytkownika/pasywnego użytkownika.
2. Na wniosek posiadacza rachunku bank może zablokować dostęp do serwisu internetowego uniemożliwiając jednocześnie możliwość dokonania transakcji.

§ 17

1. W przypadku utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia indywidualnych danych uwierzytelniających lub nieuprawnionego dostępu do serwisu internetowego jego użytkownik/pasywny użytkownik powinien go niezwłocznie zastrzec, podając swoje dane personalne.
2. Zastrzeżenie, o którym mowa w ust. 1, może być dokonane osobiście w placówce banku lub pod numerami telefonów wskazanymi i aktualizowanymi przez bank, w formie komunikatu, w placówkach banku lub na stronie internetowej banku.
3. Bank ma prawo zmiany numerów telefonów, pod którymi dokonywane są zastrzeżenia; w razie skorzystania z tego uprawnienia, bank powiadomi użytkownika/pasywnego użytkownika o dokonanej zmianie drogą elektroniczną na adres poczty elektroniczny (e-mail) wskazany przez posiadacza rachunku lub w formie komunikatu przekazanego za pośrednictwem elektronicznego kanału dostępu.
4. Zastrzeżenie, o którym mowa w ust. 1, nie może być odwołane i powoduje niemożność dalszego dostępu do serwisu internetowego.
5. W przypadku utraty indywidualnych danych uwierzytelniających oraz ich zastrzeżenia posiadacz rachunku może wystąpić z wnioskiem o wydanie nowych indywidualnych danych uwierzytelniających.
6. W przypadku utraty, kradzieży, przywłaszczenia lub stwierdzenia nieuprawnionego użycia telefonu komórkowego oznaczonego do autoryzacji lub zmiany telefonu do autoryzacji, lub zmiany numeru telefonu do autoryzacji, użytkownik jest zobowiązany dokonać zmiany danych, zgodnie z zapisami ust.7.
7. W przypadku, gdy użytkownik chce zmienić dotychczasowe dane niezbędne do otrzymywania kodów autoryzacyjnych SMS na nowe dane:
   1) jeżeli jest w posiadaniu dotychczasowego telefonu do autoryzacji, koniecznym jest dokonać zmiany danych autoryzacyjnych za pośrednictwem serwisu internetowego, o ile bank udostępnia taką funkcjonalność - bank zmienia nr telefonu do autoryzacji po kontakcie pracownika banku z klientem i weryfikacji zlecenia zmiany numeru telefonu;
   2) jeżeli nie posiada dotychczasowego numeru telefonu do autoryzacji, konieczne jest złożenie stosownej dyspozycji w placówce banku
8. Do chwili otrzymania powiadomienia, o którym mowa w ust.1, bank nie ponosi odpowiedzialności za informacje uzyskane przez osoby trzecie lub operacje wykonane przez bank na podstawie dyspozycji złożonych przez te osoby, jeżeli w wyniku nieuprawnionego użycia przez te osoby indywidualnych danych uwierzytelniających, system bankowy zidentyfikował podmiot składający oświadczenie woli, jako uprawniony do złożenia takiego oświadczenia woli zgodnie z umową.

9. Użytkownik/pasywny użytkownik ponosi odpowiedzialność za wszelkie skutki będące następstwem użycia przez osoby nieuprawnione indywidualnych danych uwierzytelniających lub niedopełnienia przez użytkownika/pasywnego użytkownika obowiązków, o których mowa w niniejszym paragrafie.

§ 18

1. Bank ma prawo do zastrzeżenia indywidualnych danych uwierzytelniających w przypadku:
   1) wygaśnięcia lub rozwiązania umowy ramowej;
   2) uzasadnionych przyczyn związanych z bezpieczeństwem indywidualnych danych uwierzytelniających tzn. powzięcia informacji o wejściu w ich posiadanie osób nieuprawnionych;
   3) podejrzenia nieuprawnionego użycia indywidualnych danych uwierzytelniających lub umyślnego doprowadzenia do nieautoryzowanej transakcji płatniczej.
2. Z zastrzeżeniem ust.3, bank informuje posiadacza rachunku o zamiarze zastrzeżenia indywidualnych danych uwierzytelniających w przypadkach określonych w ust. 1 pkt 2 i 3, przed ich zastrzeżeniem, a jeżeli nie jest to możliwe – niezwłocznie po ich zastrzeżeniu, telefonicznie lub na podany adres e-mail.
3. Bank nie przekazuje informacji o zastrzeżeniu, jeżeli jej przekazanie byłoby nieuzasadnione ze względów bezpieczeństwa lub zabronione na mocy odrębnych przepisów.

Rozdział 6 Udostępnianie informacji na potrzeby świadczenia usług inicjowania transakcji płatniczych i usług dostępu do informacji o rachunku. Potwierdzenie dostępności środków na rachunku

§ 19

1. Bank może udostępnić dostawcy świadczącemu usługi dostępu do informacji o rachunku, na podstawie wyrażonej przez użytkownika korzystającego z serwisu internetowego, zgody na dostęp do informacji o rachunku oraz transakcjach na tym rachunku.
2. Dostęp do informacji na rachunku, o którym mowa w ust 1, jest również możliwy w przypadku dostawców inicjujących transakcję płatniczą dla użytkowników korzystających z serwisu internetowego.
3. Bank na wniosek dostawcy wydającego instrumenty płatnicze oparte na karcie płatniczej, niezwłocznie potwierdza dostępność na rachunku płatniczym płatnika kwoty niezbędnej do wykonania transakcji płatniczej realizowanej w oparciu o tę kartę jeżeli:
   1) rachunek płatniczy użytkownika jest dostępny online w momencie występowania z wnioskiem oraz
   2) użytkownik udzielił bankowi zgody na udzielanie odpowiedzi na wnioski dostawcy wydającego instrumenty płatnicze oparte na karcie płatniczej dotyczące potwierdzenia, że kwota odpowiadająca kwocie określonej w transakcji płatniczej realizowanej w oparciu o tę kartę jest dostępna na rachunku płatniczym użytkownika, oraz
   3) zgoda, o której mowa w pkt 2, została udzielona przed wystąpieniem z pierwszym wnioskiem dotyczącym potwierdzenia.
4. Dostawca wydający instrumenty płatnicze oparte na karcie płatniczej może wystąpić z wnioskiem, o którym mowa w ust. 3, jeżeli:
   1) użytkownik udzielił temu dostawcy zgody na występowanie z wnioskiem, o którym mowa w ust. 3, oraz
   2) użytkownik zainicjował transakcję płatniczą realizowaną w oparciu o kartę płatniczą na daną kwotę przy użyciu instrumentu płatniczego opartego na tej karcie wydanego przez danego dostawcę, oraz
   3) dostawca uwierzytelni siebie wobec banku przed złożeniem wniosku, o którym mowa w ust. 3, oraz w sposób bezpieczny porozumiewa się z bankiem.
5. Potwierdzenie, o którym mowa w ust. 3, polega na udzieleniu odpowiedzi „tak” albo „nie” i nie obejmuje podania salda rachunku; odpowiedzi nie przechowuje się ani nie wykorzystuje do celów innych niż wykonanie transakcji płatniczej realizowanej w oparciu o kartę płatniczą.
6. Potwierdzenie, o którym mowa w ust. 3, nie umożliwia bankowi dokonania blokady środków pieniężnych na rachunku płatniczym użytkownika.
7. Użytkownik może zwrócić się do banku o przekazanie mu danych identyfikujących dostawcę, o którym mowa w ust. 4, oraz udzielonej odpowiedzi, o której mowa w ust. 5.
8. Bank może odmówić dostawcy świadczącemu usługę dostępu do informacji o rachunku lub dostawcy świadczącemu usługę inicjowania transakcji płatniczej dostępu do danego rachunku płatniczego z obiektywnie uzasadnionych i należycie udokumentowanych przyczyn, związanych z nieuprawnionym lub nielegalnym dostępem do rachunku przez takiego dostawcę, w tym nieuprawnionym zainicjowaniem transakcji płatniczej. W takim przypadku bank w uzgodniony sposób informuje płatnika o odmowie dostępu do rachunku i jej przyczynach. Informacja ta, o ile

jest to możliwe, przekazywana jest płatnikowi przed odmową dostępu, a najpóźniej bezzwłocznie po takiej odmowie, nie później jednak niż w dniu roboczym następującym po dniu takiej odmowy, chyba że jej przekazanie nie byłoby wskazane z obiektywnie uzasadnionych względów bezpieczeństwa lub jest sprzeczne z odrębnymi przepisami. Bank umożliwia dostawcy świadczącemu usługę dostępu do informacji o rachunku oraz dostawcy świadczącemu usługę inicjowania transakcji płatniczej dostęp do rachunku płatniczego niezwłocznie po ustaniu przyczyn uzasadniających odmowę.

Rozdział 7 Standardowy limit pojedynczej operacji

§ 20

1. Standardowy limit pojedynczej operacji dokonywanej za pośrednictwem bankowości elektronicznej.

Limit pojedynczej operacji
100.000 złotych

2. W przypadku operacji dokonywanych z rachunków w walucie innej niż PLN, kwota limitu przeliczana jest wg kursu średniego z dnia wykonania operacji.
3. Z zastrzeżeniem ust. 4 posiadacz rachunku może wnioskować o indywidualne ustalenie limitów, o których mowa w ust. 1.
4. O wysokości limitów ostatecznie decyduje bank.

Rozdział 8 Inne postanowienia

§ 21

Użytkownik zobowiązany jest do nieprzekazywania za pośrednictwem serwisu internetowego treści o charakterze bezprawnym (zakaz).