

Zasady udostępniania i funkcjonowania elektronicznych kanałów dostępu

Rozdział 1. Udostępnienie i warunki korzystania z elektronicznych kanałów dostępu

§ 1

1. Bank może świadczyć użytkownikom usługi w zakresie obsługi produktów i usług za pośrednictwem elektronicznych kanałów dostępu:
 - 1) w ramach bankowości elektronicznej – usługi zapewniające dostęp do informacji o produktach i usługach banku oraz składanie dyspozycji poprzez:
 - a) bankowość internetową (serwis internetowy/serwis Internet Banking) – dostęp i dyspozycje składane na komputerze lub urządzeniu mobilnym przy użyciu przeglądarki internetowej;
 - b) bankowość mobilną – dostęp i dyspozycje składane przy użyciu zaufanego urządzenia mobilnego za pomocą aplikacji mobilnej;
 - 2) powiadomień SMS (serwis SMS) – uzyskiwanie informacji związanych z transakcjami na rachunku w formie wiadomości SMS.
2. Warunki korzystania z bankowości elektronicznej określa Przewodnik dla klienta publikowany na stronie internetowej banku; Przewodnik dla klienta stanowi instrukcję użytkowania zawierającą opis elektronicznych kanałów dostępu, wymagania techniczne dla tego kanału i zasady prawidłowego posługiwania się kanałem przez klienta
3. Informacje o aktualnej ofercie usług dostępnych w aplikacji mobilnej SGB Mobile opisano w Regulaminie korzystania z aplikacji mobilnej SGB Mobile, zamieszczonym na stronie internetowej banku

§ 2

1. Elektroniczne kanały dostępu mogą być udostępnione wyłącznie klientom posiadającym rachunek oszczędnościowo-rozliczeniowy lub podstawowy rachunek płatniczy, chyba że Regulamin korzystania z aplikacji mobilnej SGB Mobile stanowi inaczej.
2. Użytkownikiem bankowości internetowej może być posiadacz rachunku, współposiadacz rachunku oraz pełnomocnik, któremu udzielono pełnomocnictwa stałego. Młodociany korzysta z elektronicznych kanałów dostępu na podstawie zgody przedstawiciela ustawowego, w ramach zawartej z bankiem umowy.
3. Użytkownik może wnioskować o udostępnienie kolejnych produktów lub usług, zmianę warunków świadczenia tych produktów lub usług i zawierać umowy za pośrednictwem elektronicznych kanałów dostępu, o ile taki sposób zawierania umów został udostępniony przez bank; informacje o ofercie oraz dostępnych sposobach zawierania umów zawarte są na stronie internetowej banku oraz w Przewodniku dla klienta.

§ 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 stałym do rachunku innego klienta z uwzględnieniem limitów transakcji, o których mowa w § 19.

§ 4

1. W przypadku dokonywania transakcji użytkownikowi zaleca się:
 - 1) korzystanie z zaufanych komputerów posiadających aktualne oprogramowanie antywirusowe;
 - 2) sprawdzić, czy transmisja jest szyfrowana protokołem SSL (ang. Secure Socket Layer), który zapewnia poufność i integralność transmisji danych;
 - 3) nie korzystać z otwartych i niezabezpieczonych sieci.
2. Szczegółowy opis środków bezpieczeństwa, jakie powinien przedsięwziąć użytkownik w celu zapewnienia bezpieczeństwa korzystania z elektronicznych kanałów dostępu znajduje się w Przewodniku dla klienta oraz na stronie internetowej banku.
3. Warunkiem korzystania z usługi przez użytkownika 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 ma obowiązek korzystać z bankowości internetowej zgodnie z umową i regulaminem, zabezpieczyć otrzymane indywidualne dane uwierzytelniające przed dostępem do nich osób trzecich i zapewnić ich poufność.
2. Z chwilą otrzymania indywidualnych danych uwierzytelniających, o których mowa w ust. 1, użytkownik podejmuje niezbędne środki zapobiegające naruszeniu indywidualnych danych uwierzytelniających; ze względów bezpieczeństwa poszczególnych danych nie wolno przechowywać razem z sobą.
3. Bank zapewnia użytkownikowi należyłą ochronę indywidualnych danych uwierzytelniających; indywidualne dane uwierzytelniające są dostępne wyłącznie użytkownikom uprawnionym do korzystania z nich.

§ 6

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

Rozdział 2. Dyspozycje składane za pośrednictwem elektronicznych kanałów dostępu

§ 7

Wszelkie oświadczenia woli składane w postaci elektronicznej przez użytkownika bankowi, 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.

§ 8

1. Do dysponowania rachunkami za pośrednictwem elektronicznych kanałów dostępu mają zastosowanie ogólne zasady dotyczące dysponowania rachunkami, określone w rozdziale 2 regulaminu oraz dotyczące poszczególnych rodzajów rachunków, o których mowa w rozdziale 4 regulaminu, z zastrzeżeniem postanowień § 9-12 niniejszego załącznika oraz sposobu posługiwania się elektronicznym kanałem dostępu opisanym w instrukcji użytkownika.
2. Bank w bankowości internetowej umożliwia użytkownikowi:
 - 1) składanie wniosku o wypłatę świadczenia wychowawczego w ramach Programu Rodzina 800+ wraz z załącznikami oraz programu Dobry start – dostępność usługi uzależniona jest od współpracy z Ministerstwem Rodziny, Pracy i Polityki Społecznej;
 - 2) usługę identyfikacji elektronicznej SGB ID;
 - 3) składanie innych wniosków udostępnionych przez bank, w tym dotyczących produktów lub usług podmiotów trzecich współpracujących z bankiem.
3. Bank świadczy usługę oferowaną przez integratorów płatności internetowych, którzy inicjują płatności w formie przelewów typu pay by link we współpracy z bankiem, 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.
4. Zgody na wykonanie transakcji płatniczej użytkownik może udzielić również za pośrednictwem dostawcy świadczącego usługę inicjowania transakcji płatniczej.
5. W przypadku inicjowania transakcji przez dostawcę świadczącego usługę inicjowania transakcji lub przez odbiorcę lub za jego pośrednictwem, użytkownik nie może odwołać zlecenia płatniczego po udzieleniu dostawcy świadczącemu usługę inicjowania transakcji zgody na zainicjowanie transakcji albo po udzieleniu odbiorcy zgody na wykonanie transakcji.

§ 9

1. Wszelkie dyspozycje i zlecenia płatnicze w bankowości elektronicznej, użytkownik składa bankowi w formie elektronicznej, po jego uwierzytelnieniu, w sposób umożliwiający bankowi jego identyfikację i zapoznanie się z treścią dyspozycji; dyspozycje, o których mowa w zdaniu

- pierwszym spełniają wymagania formy pisemnej w zakresie, w jakim mają związek z czynnościami bankowymi, przy czym wybrane dyspozycje złożone przez małoletniego, który nie ukończył 13 roku życia są realizowane po ich zatwierdzeniu w bankowości mobilnej przez przedstawiciela ustawowego¹.
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. 1 i 3.
 3. Bank stosuje silne uwierzytelnianie, w przypadku, gdy 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 niewymagających silnego uwierzytelniania, wskazanych w ust. 4.
 4. Bank może nie stosować silnego uwierzytelniania w następujących przypadkach:
 - 1) dostępu 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 jest wpisany na listę zaufanych odbiorców uprzednio utworzoną przez użytkownika, przy zastosowaniu silnego uwierzytelniania;
 - 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 z zastosowaniem silnego uwierzytelniania;
 - 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 przez użytkownika transakcji płatniczej, którą bank uzna za charakteryzującą się niskim poziomem ryzyka, zgodnie z mechanizmem monitorowania transakcji banku.
 5. Bank stosuje silne uwierzytelnianie użytkownika, jeżeli spełniony jest którykolwiek z następujących warunków:
 - 1) 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 po raz ostatni uzyskał dostęp do informacji określonych w ust. 4 pkt 1 lit. b w trybie online oraz odkąd ostatni raz zastosowano silne uwierzytelnianie użytkownika.
 6. Bank zastrzega sobie prawo kontaktu z użytkownikiem w celu realizacji zlecenia płatniczego.
 7. Dostęp użytkownika do serwisu internetowego następuje poprzez podanie identyfikatora użytkownika i hasła.
 8. Hasło, o którym mowa w ust. 7 jest nadawane przez użytkownika (podczas procesu pierwszego logowania lub podczas odblokowania dostępu do bankowości internetowej) po otrzymaniu z banku hasła tymczasowego. Bank określa w Przewodniku dla klienta zasady tworzenia hasła (składniki hasła).
 9. Autoryzacja dyspozycji składanych za pośrednictwem serwisu internetowego odbywa się poprzez użycie indywidualnych danych uwierzytelniających tj. hasła SMS lub aplikacji mobilnej (wymogi oraz zasady dotyczące instalacji aplikacji na urządzeniu mobilnym i sposób jego aktywacji przez użytkownika opisane są w Przewodniku użytkownika aplikacji), z zastrzeżeniem ust. 10.
 10. Jeżeli użytkownik, podczas procesu logowania 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 kodów SMS lub aplikacji mobilnej.² Urządzeniem

¹ po wdrożeniu funkcjonalności przez bank

² na okres nie dłuższy niż 90 dni

zaufanym może być np. prywatny komputer, smartfon lub tablet, z którego korzysta wyłącznie użytkownik. Bank podczas procesu logowania weryfikuje określone cechy tego urządzenia.

11. Użytkownik w dowolnym momencie ma możliwość, poprzez bankowość internetową, usunięcia swojego urządzenia zaufanego, a każde kolejne logowanie do bankowości internetowej będzie wymagało dodatkowego potwierdzania kodem otrzymywanym wiadomością SMS.
12. Autoryzacja dokonana przez użytkownika jest równoznaczna z poleceniem bankowi dokonania określonej czynności i stanowi podstawę jej dokonania.
13. Bank przesyła kody SMS wykorzystywane przy stosowanych metodach uwierzytelniania na numer telefonu komórkowego wskazany przez użytkownika w umowie, karcie informacyjnej lub pełnomocnictwie.
14. Bank może wprowadzić, wycofać oraz zmienić rodzaj stosowanych indywidualnych danych uwierzytelniających poprzez udostępnienie ich użytkownikowi oraz zawiadomienie użytkownika o dokonanej zmianie; informacja o stosowanych indywidualnych danych uwierzytelniających jest zamieszczona w Przewodniku dla klienta 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 jakiegokolwiek 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 drogą elektroniczną, przy czym użytkownik zobowiązuje się stosować zasady autoryzacji obowiązujące dla danego elektronicznego kanału dostępu.
2. Autoryzowane zlecenie płatnicze nie może zostać odwołane, za wyjątkiem sytuacji określonych w § 27 ust.5 regulaminu.

§ 12

1. Przyjęcie do realizacji dyspozycji złożonej przez bankowość internetową bank potwierdza w formie informacji wysyłanej poprzez ten kanał.
2. W przypadku nieprzyjęcia przez bank dyspozycji złożonej za pośrednictwem bankowości internetowej z powodu:
 - 1) jej niekompletności;
 - 2) złożenia dyspozycji sprzecznych ze sobą;
 - 3) podania nieprawidłowego numeru rachunku odbiorcy;
 - 4) braku środków pieniężnych do realizacji dyspozycji lub
 - 5) innych okoliczności uniemożliwiających jej przyjęcie przez bankużytkownik otrzyma za pośrednictwem bankowości elektronicznej informację o fakcie i przyczynie niezrealizowania dyspozycji w formie komunikatu elektronicznego lub od pracownika placówki banku.

Rozdział 3. Korzystanie z usług bankowości elektronicznej

§ 13

1. Bank zapewnia posiadaczowi dostęp do elektronicznych kanałów dostępu 7 dni w tygodniu 24 godziny na dobę, z zastrzeżeniem ograniczeń wskazanych w § 14.
2. Za pośrednictwem elektronicznych kanałów dostępu użytkownik uzyskuje dostęp do wszystkich rachunków otwartych przed dniem aktywowania usługi oraz do rachunków otwartych w terminie późniejszym.

Rozdział 4. Ograniczenia w korzystaniu z usług bankowości elektronicznej

§ 14

1. Bank jest zobowiązany zablokować dostęp do serwisu internetowego uniemożliwiając tym samym wykonanie transakcji w jednym z następujących przypadków:
 - 1) złożenia przez użytkownika dyspozycji zablokowania dostępu do bankowości internetowej;
 - 2) zastrzeżenia przez użytkownika środka identyfikacji elektronicznej;
 - 3) kolejnego trzykrotnego wpisania nieprawidłowego hasła dostępu lub kodu SMS;

- 4) zalogowania się do systemu z innego kraju przed upływem określonego czasu od ostatniego logowania z poprzedniego kraju (blokada lokalizacyjna/geograficzna);
- 5) zalogowania się do systemu 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 serwisu internetowego 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 serwisu internetowego niezgodnie z zasadami bezpieczeństwa określonymi w niniejszym załączniku lub w sposób zagrażający bezpieczeństwu korzystania z serwisu internetowego;
 - 4) dokonywania czynności konserwacyjnych w serwisie internetowym lub innym systemie teleinformatycznym, związanym z wykonaniem umowy, o czym z wyprzedzeniem bank poinformuje klienta na stronie internetowej banku;
 - 5) dokonywania czynności służących usunięciu awarii, usterek lub nieprawidłowości działania serwisu internetowego lub innych systemów teleinformatycznych, związanych z wykonaniem umowy;
 - 6) wymiany stosowanych indywidualnych danych uwierzytelniających, o czym z wyprzedzeniem bank poinformuje użytkownika pisemnie lub na stronie internetowej banku;
 - 7) uzasadnionego podejrzenia, iż transakcje na rachunku użytkownika mają związek z popełnieniem przestępstwa związanego z praniem pieniędzy lub finansowaniem terroryzmu;
 - 8) gdy na rachunku klienta wystąpi zamrożenie wartości majątkowych lub gdy wobec klienta należy stosować sankcje międzynarodowe lub embarga;
 - 9) braku możliwości zastosowania środków bezpieczeństwa finansowego, w tym braku aktualnego dokumentu tożsamości klienta lub osób upoważnionych do działania w jego imieniu.
3. Bank może uchylić ograniczenie albo blokadę dostępu do serwisu internetowego w przypadku, o którym mowa w ust. 2 pkt 1, na wniosek złożony przez posiadacza rachunku lub pełnomocnika stałego, w sposób wskazany w ust. 4; w takim przypadku bank wydaje użytkownikowi nowe indywidualne dane uwierzytelniające lub uchyli ograniczenia, lub blokady przy zachowaniu dotychczasowych indywidualnych danych uwierzytelniających.
4. W przypadkach, o których mowa w ust. 2 pkt 1 uchylenie:
 - 1) ograniczenia lub blokady dostępu do serwisu internetowego - następuje na podstawie dyspozycji klienta złożonej telefonicznej lub w siedzibie, lub dowolnej placówce banku;
 - 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 posiadacza rachunku 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. Zastrzeżenie środków identyfikacji elektronicznej

§ 15

1. Dostęp do serwisu internetowego oraz możliwość posługiwania się indywidualnymi danymi uwierzytelniającymi może zostać zastrzeżony przez:
 - 1) bank, zgodnie z postanowieniami § 17;

- 2) użytkownika;
- 3) przedstawiciela ustawowego małoletniego.
2. Na wniosek posiadacza rachunku bank może zablokować dostęp do serwisu internetowego uniemożliwiając jednocześnie dokonanie transakcji.

§ 16

1. W przypadku utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia indywidualnych danych uwierzytelniających lub nieuprawnionego dostępu do serwisu internetowego użytkownik/przedstawiciel ustawowy małoletniego powinien niezwłocznie telefonicznie dokonać jego zastrzeżenia, 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, blokowanie dostępu do serwisu internetowego, o czym bank powiadomi użytkownika drogą elektroniczną na adres poczty elektronicznej (e-mail) wskazany przez posiadacza rachunku lub w formie komunikatu przekazanego za pośrednictwem serwisu internetowego.
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 lub działający w jego imieniu przedstawiciel ustawowy może wystąpić z wnioskiem o wydanie nowego indywidualnych danych uwierzytelniających.
6. W przypadku utraty kradzieży, przywłaszczenia lub stwierdzenia nieuprawnionego użycia telefonu komórkowego, który jest powiązany z numerem telefonu oznaczonym, jako telefon 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 SMS na nowe dane:
 - 1) jeżeli jest w posiadaniu dotychczasowego numeru telefonu do autoryzacji, może dokonać zmiany numeru telefonu za pośrednictwem serwisu internetowego, jeśli bank udostępni taką funkcjonalność - bank może skontaktować się z użytkownikiem celem weryfikacji zlecenia zmiany numeru tego telefonu i zmienia nr telefonu;
 - 2) jeśli nie posiada dotychczasowego telefonu do autoryzacji, konieczne jest złożenie stosownej dyspozycji w placówce banku.

§ 17

1. Bank ma prawo zastrzec indywidualne dane uwierzytelniające w przypadku:
 - 1) wygaśnięcia lub rozwiązania umowy;
 - 2) uzasadnionych przyczyn związanych z bezpieczeństwem indywidualnych danych uwierzytelniających tzn. powzięcia informacji o wejściu w ich posiadanie osób trzecich;
 - 3) podejrzenia nieuprawnionego użycia indywidualnych danych uwierzytelniających lub umyślnego doprowadzenia do nieautoryzowanej transakcji płatniczej.
2. Z zastrzeżeniem ust. 3, bank informuje posiadacza 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 jego zastrzeżeniu, telefonicznie.
3. Bank nie przekazuje informacji o zastrzeżeniu, jeżeli przekazanie tej informacji 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

§ 18

1. Bank, na podstawie zgody użytkownika korzystającego z serwisu internetowego, udostępni dostawcy świadczącemu usługi dostępu do informacji o rachunku, dostęp do informacji o rachunku oraz transakcjach na tym rachunku.

2. Dostęp do informacji o 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 płatnika (użytkownika) jest dostępny online w momencie występowania z wnioskiem oraz
 - 2) płatnik (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 serwisu internetowego zainicjował transakcję płatniczą realizowaną w oparciu o kartę płatniczą na daną kwotę przy użyciu instrumentu płatniczego opartego na tej karcie wydanej przez danego dostawcę oraz
 - 3) dostawca uwierzył w siebie wobec banku przed złożeniem wniosku, o którym mowa w ust. 3, oraz porozumiewa się z bankiem w sposób bezpieczny.
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 płatnika.
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 dokonywanej za pośrednictwem bankowości elektronicznej

§ 19

1. Standardowe limity pojedynczej operacji oraz limity wszystkich transakcji w ciągu dnia dokonywanych za pośrednictwem serwisu internetowego na rachunku (w jednostkach waluty, w której prowadzony jest dany rachunek) wynoszą:

Waluta rachunku	Limit pojedynczej operacji/ Limit wszystkich transakcji w ciągu dnia
złoty polski	10 000
funt brytyjski	2 000
dolar amerykański	2 000
euro	2 000

2. W przypadku wprowadzenia do oferty rachunku w walucie innej niż wskazana w ust. 1, standardowy limit pojedynczej operacji wyznacza się jako iloraz odpowiedniego limitu w złotych i kursu średniego NBP nowej waluty, z poprzedniego dnia roboczego, poprzedzającego dzień otwarcia rachunku.
3. Z zastrzeżeniem ust. 4 użytkownik, może wnioskować o indywidualne ustalenie limitów, o których mowa w ust. 1.
4. O wysokości limitów ostatecznie decyduje bank.

Rozdział 8. Inne postanowienia

§ 20

1. Użytkownik zobowiązany jest do nieprzekazywania za pośrednictwem serwisu internetowego treści o charakterze bezprawnym.
2. Zabronione jest wykorzystywanie serwisu internetowego do popełniania, pomagania w popełnianiu lub podżegania do popełniania czynów zabronionych, w szczególności do wprowadzania do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł.