Załącznik nr 3
do „Regulaminu świadczenia usług
w zakresie prowadzenia rachunków
bankowych dla klientów instytucjonalnych”

Zasady udostępniania i funkcjonowania elektronicznych kanałów dostępu

Rozdział 1. Udostępnienie i warunki korzystania z usług bankowości elektronicznej

§ 1

1. Bank może świadczyć usługi w zakresie obsługi produktów i usług za pośrednictwem następujących elektronicznych kanałów dostępu:
   1) w ramach bankowości elektronicznej:
      a) bankowość internetowa (serwis internetowy) - dostęp do rachunku poprzez sieć internet;
      b) bankowość mobilna - dostęp do rachunku za pomocą aplikacji mobilnej Nasz Bank
   2) powiadomienia SMS (serwis SMS Banking)- uzyskiwanie informacji związanych z operacjami
      na rachunku w formie wiadomości SMS.
2. Wykaz usług dostępnych za pośrednictwem bankowości elektronicznej oraz warunki korzystania z usług określają:
   a) Instrukcja użytkownika *„Internetowa obsługa rachunku”* stanowi instrukcję użytkowania zawierającą opis bankowości internetowej (serwis internetowy), wymagania techniczne i zasady prawidłowego posługiwania się tym dostępem poprzez sieć internet przez klienta;
   b) Przewodnik użytkownika Aplikacja mobilna Nasz Bank stanowi instrukcję użytkowania zawierającą opis bankowości mobilnej, wymagania techniczne i zasady prawidłowego posługiwania się aplikacją mobilną przez klienta;

   publikowane na stronie internetowej banku – www.bsstarabiala.pl.
3. Kanał www, o którym mowa w ust. 1 pkt 1, jest dostępny w dwóch wariantach:
   1) INTERNET BANKING - z jednoosobową autoryzacją dyspozycji, z zastosowaniem wymaganych przez Bank metod uwierzytelniania ;
   2) INTERNET BANKING DLA FIRM - z jedno lub wieloosobową autoryzacją dyspozycji, z zastosowaniem wymaganych przez Bank metod uwierzytelniania.

§ 2

1. Usługi bankowości elektronicznej mogą być udostępniane wyłącznie w przypadku posiadania przez posiadacza rachunku bieżącego prowadzonego w złotych; Bank może udostępnić elektroniczne kanały dostępu dla posiadaczy innych rachunków bez wymogu posiadania wyżej wymienionych produktów, o czym poinformuje na stronie internetowej Banku.
2. Posiadacz rachunku może wnioskować o udostępnienie kolejnych usług i zawierać umowy za pośrednictwem elektronicznych kanałów dostępu o ile taki sposób został

udostępniony przez Bank; informacje o ofercie oraz dostępnych sposobach zawierania umów zawarte są na stronie internetowej Banku.

§ 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, o których mowa w Rozdziale 7 niniejszych zasad.

§ 4

1. W przypadku korzystania i dokonywania transakcji z wykorzystaniem bankowości elektronicznej:
   1) zaleca się korzystanie z zaufanych komputerów, urządzeń mobilnych posiadających aktualne oprogramowanie antywirusowe;
   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 do bankowości elektronicznej; 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 dla klienta /Instrukcja użytkownika„ ‘Internetowa obsługa rachunku”,/ i Przewodnikiem użytkownika Aplikacja mobilna Nasz Bank oraz zabezpieczyć otrzymane indywidualne dane uwierzytelniające przed dostępem osób nieuprawnionych i zapewnienia ich poufności.
2. Użytkownik/pasywny użytkownik uzyskuje dostęp do rachunku za pomocą udostępnionych mu indywidualnych danych uwierzytelniających
3. Z chwilą otrzymania indywidualnych danych uwierzytelniających, użytkownik /pasywny użytkownik podejmuje niezbędne środki służące zapobieżeniu naruszenia indywidualnych danych uwierzytelniających, w szczególności że przyjmuje do wiadomości, że ze względów bezpieczeństwa poszczególnych indywidualnych danych uwierzytelniających nie wolno przechowywać 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 usługi przez Bank wymaga zachowania warunków i trybu przewidzianego dla zmiany regulaminu.

Rozdział 2. Dyspozycje składane za pośrednictwem elektronicznych kanałów dostępu

§ 7

Wszelkie oświadczenia woli składane wobec Banku przez użytkownika w postaci elektronicznej będą ważne i wiążące pod względem prawnym dla posiadacza rachunku i Banku, jeżeli przy użyciu środków identyfikacji elektronicznej dokonana została poprawna identyfikacja użytkownika składającego oświadczenie woli, z zastosowaniem wymaganych przez Bank metod uwierzytelniania, przy uwzględnieniu wymogów silnego uwierzytelniania.

§ 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 danym elektronicznym kanałem dostępu opisanym Instrukcją użytkownika „Internetowa obsługa rachunku" oraz Przewodnikiem użytkownika Aplikacji mobilnej Nasz Bank .
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 nie może autoryzować dyspozycji.
6. Bank umożliwia składanie w serwisie internetowym wybranych wniosków.

§ 9

1. Wszelkie dyspozycje i zlecenia płatnicze w bankowości elektronicznej, użytkownik składa Bankowi w postaci elektronicznej, po jego uwierzytelnieniu, w sposób umożliwiający Bankowi jego identyfikację i zapoznanie się z treścią dyspozycji; wyżej wymienione dyspozycje spełniają wymagania formy pisemnej w zakresie, w jakim mają związek z czynnościami bankowymi.
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 on-line;
   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;
   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 tego samego dostawcę usług płatniczych prowadzącego rachunek;
   5) inicjowania zdalnej transakcji, którą Bank uzna za charakteryzującą się nikim 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/pasywny 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/pasywnego użytkownika.
6. Bank zastrzega sobie prawo skontaktowania się z użytkownikiem w celu realizacji zlecenia płatniczego.
7. Dostęp użytkownika do:
   1) serwisu internetowego następuje poprzez podanie identyfikatora użytkownika, hasła stałego oraz::
   a) udostępnionych użytkownikowi indywidualnych danych uwierzytelniających o których mowa w ust. 8 lub,
   b) logowania na urządzeniu zaufanym przy użyciu metody DFP,
   2) Aplikacji mobilnej Nasz Bank następuje poprzez:
   a) autoryzacje e-Pin lub
   b) z wykorzystaniem cech biometrycznych - odcisk palca, Face ID[6].
8. Autoryzacja dyspozycji składanych za pośrednictwem bankowości elektronicznej (serwisu internetowego) przez użytkownika/pasywnego użytkownika odbywa się po

[6] W przypadku wdrożenia ww. funkcjonalności Bank zamieści stosowną informacje na swojej stronie internetowej .

zalogowaniu udostępnionym przez Bank środkiem identyfikacji elektronicznej poprzez podanie następujących danych uwierzytelniających:

1) dla wariantu – INTERNET BANKING, o którym mowa w § 1 ust. 4 pkt 1 poprzez:
a) kod wysłany SMS wraz z kodem uwierzytelnienia[7]
b) mobilnej autoryzacji w aplikacji mobilnej Nasz Bank;
c) token Vasco lub token Vasco z PIN lub token Vasco z klawiaturą.
2) dla wariantu INTERNET BANKING DLA FIRM, o którym mowa w § 1 ust. 4 pkt 2 poprzez użycie:
a) kod wysłany SMS wraz z kodem uwierzytelnienia
b) mobilnej autoryzacji token Vasco lub token Vasco z PIN lub token Vasco z klawiaturą
c) aplikacja nPodpis wraz z certyfikatem (Athena, Cryptocard lub do podpisu kwalifikowanego)

chyba że Bank udostępni inne środki identyfikacji elektronicznej, które są opisane w Przewodniku dla klienta /Instrukcji użytkownika „Internetowa obsługa rachunku".

9. Autoryzacja dokonana przez użytkownika jest równoznaczna z poleceniem Bankowi dokonania określonej czynności i stanowi podstawę jej dokonania.
10. Bank przesyła kody autoryzacyjne wykorzystywane przy stosowanych metodach uwierzytelniania na numer telefonu komórkowego, który użytkownik wskazał w umowie, karcie informacyjnej lub pełnomocnictwie.
11. 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 rodzajach stosowanych indywidualnych danych uwierzytelniających jest zamieszczona w Instrukcji użytkownika „Internetowa obsługa rachunku", w Przewodniku użytkownika „Aplikacji mobilnej Nasz Bank" 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 na drodze elektronicznej, przy czym użytkownik zobowiązuje się do stosowania zasad autoryzacji obowiązujących dla tego elektronicznego kanału dostępu.
2. Autoryzowane zlecenie płatnicze nie może zostać odwołane, za wyjątkiem sytuacji o których mowa 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:

[7] Kod uwierzytelnienia ustawiany jest indywidualnie przez klienta banku w bankowości internetowej i jest oprócz kodu SMS kodem dedykowanym dla operacji potwierdzanych poprzez SMS. Po otrzymaniu kodu SMS klient w bankowości internetowej oprócz wpisania kodu SMS musi wpisać także kod uwierzytelnienia.

1) jej niekompletności;
2) złożenia dyspozycji sprzecznych ze sobą;
3) podania nieprawidłowego numeru rachunku odbiorcy;
4) braku środków pieniężnych dla realizacji dyspozycji;
5) lub innych okoliczności uniemożliwiających jej przyjęcie przez Bank,

użytkownik/pasywny użytkownik otrzyma za pośrednictwem elektronicznego kanału dostępu informację o fakcie i przyczynie niezrealizowania dyspozycji w formie właściwej dla danego elektronicznego kanału dostępu lub od pracownika placówki Banku.

§ 13

1. Bank ma prawo odmowy wykonania dyspozycji złożonej i uwierzytelnionej w bankowości elektronicznej w przypadku:
   1) gdy zaistniałe okoliczności uzasadniają wątpliwości, co do:
   a) złożenia lub autoryzacji dyspozycji przez użytkownika,
   b) zgodności dyspozycji z obowiązującymi przepisami prawa;
   2) gdy 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 elektronicznych kanałów dostępu, w przypadku wystąpienia ważnych okoliczności uniemożliwiających wykonanie tych dyspozycji, tj., 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 oograniczony dostęp do rachunków, za pośrednictwem elektronicznych kanałów dostępu.

Rozdział 4. Ograniczenia w korzystaniu z usług bankowości elektronicznej

§ 15

1. Bank jest zobowiązany zablokować dostęp do serwisu internetowego, uniemożliwiając tym samym wykonanie transakcji w jednym z następujących przypadków:
   1) złożenia przez użytkownika/pasywnego użytkownika dyspozycji zablokowania dostępu do serwisu internetowego;
   2) złożenia przez użytkownika dyspozycji dezaktywacji Aplikacji Mobilnej Nasz Bank;
   3) kolejnego trzykrotnego wpisania nieprawidłowego PIN do SGB Mobile lub hasła stałego.

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 tzn. uzyskania informacji, iż dyspozycje w serwisie internetowym składane są przez osoby nieuprawnione;

2) podejrzenia nieuprawnionego użycia indywidualnych danych uwierzytelniających lub umyślnego doprowadzenia do nieautoryzowanej transakcji płatniczej;
3) powzięcia informacji o zagrożeniu bezpieczeństwa dyspozycji;
4) dokonywania czynności konserwacyjnych serwisu internetowego 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 serwisu internetowego 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.

3. Bank może uchylić ograniczenie albo blokadę dostępu do serwisu internetowego w przypadku, o którym mowa w ust. 2 pkt 1, jeżeli na wniosek złożony przez posiadacza rachunku, Bank wyda użytkownikowi nowe indywidualne dane uwierzytelniające.
4. W przypadkach, o których mowa w ust. 2 pkt 2-6, ograniczenie lub blokada dostępu do serwisu internetowego i/lub czasowa blokada dyspozycji następuje przez możliwie krótki okres niezbędny do usunięcia przyczyny ograniczenia lub blokady.
5. W przypadkach, o których mowa w ust. 2 pkt 2-3 uchylenie:
   1) ograniczenia lub blokady dostępu do serwisu internetowego 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.

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 dokonywanie transakcji przez wszystkich użytkowników.

§ 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 telefonicznie zastrzec, podając swoje dane personalne:

2. Zastrzeżenia, o którym mowa w ust. 1, można dokonywać osobiście w placówce Banku oraz za pośrednictwem Call Center lub pod innymi 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 elektronicznej

(e-mail) wskazany przez posiadacza rachunku lub w formie komunikatu przekazanego za pośrednictwem właściwego 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, który jest oznaczony jako telefon do autoryzacji lub zmiany numeru telefonu do autoryzacji, użytkownik jest zobowiązany do złożenia stosownej dyspozycji w placówce Banku.
7. W przypadku utraty kradzieży, przywłaszczenia lub stwierdzenia nieuprawnionego użycia urządzenia, na którym jest zainstalowana aplikacja mobilna Nasz Bank służąca do autoryzacji, użytkownik jest zobowiązany do dokonania zmiany danych zgodnie z zapisami ust. 8.
8. W przypadku, gdy użytkownik chce zmienić dotychczasowe urządzenie na nowe, na którym zainstalowana jest aplikacja mobilna Nasz Bank:
   1) jeżeli jest w posiadaniu dotychczasowego urządzenia, może dokonać zmiany za pośrednictwem serwisu internetowego,
   2) jeżeli nie posiada dotychczasowego urządzenia, konieczne jest złożenie stosownej dyspozycji w placówce Banku.
9. 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 środków identyfikacji elektronicznej, system bankowy zidentyfikował podmiot składający oświadczenie woli, jako uprawniony do złożenia takiego oświadczenia woli zgodnie z umową.
10. Użytkownik/pasywny użytkownik ponosi odpowiedzialność za wszelkie skutki będące następstwem użycia przez osoby nieuprawnione środków identyfikacji elektronicznej lub niedopełnienia przez użytkownika/pasywnego użytkownika obowiązków, o których mowa w niniejszym paragrafie.

§ 18

1. Bank ma prawo zastrzec indywidualne dane uwierzytelniające:
   1) w przypadku wygaśnięcia lub rozwiązania umowy;
   2) z 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. 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 lub faksem.
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. Potwierdzanie 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 płatnika (użytkownika) jest dostępny on-line 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 serwisu internetowego 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 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, jest przekazywana 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. Standardowe limity pojedynczej operacji oraz limity wszystkich operacji w ciągu dnia

§20

1. Standardowe limity pojedynczej operacji oraz limity wszystkich operacji w ciągu dnia dokonywanych za pośrednictwem serwisu internetowego.

Limit pojedynczej operacji	Limit wszystkich operacji w ciągu dnia
200.000 złotych	300.000 złotych

2. Standardowe limity maksymalnej kwoty pojedynczej operacji i dziennego limitu operacji dokonywanych przy użyciu aplikacji mobilnej Nasz Bank.

Limit pojedynczej operacji	Limit wszystkich operacji w ciągu dnia
200.000 złotych	300.000 złotych

3. W chwili udostępniania limity dzienne przelewów przy użyciu aplikacji mobilnej Nasz Bank wynoszą:
   1) Limit pojedynczej operacji - 300 zł
   2) Limit wszystkich operacji w ciągu dnia – 1000,00 zł
4. Limity dotyczą operacji na rachunku. W przypadku operacji dokonywanych z rachunków w walucie obcej, innej niż PLN, kwota limitu przeliczana jest wg kursu średniego z dnia wykonania operacji.
5. Z zastrzeżeniem ust. 4 Posiadacz rachunku może wnioskować o indywidualne ustalenie limitów, o których mowa w ust. 1.
6. O wysokości limitów ostatecznie decyduje Bank.
7. Standardowy limit w usłudze Smart Wypłata pojedynczej transakcji w ciągu dnia zlecanej za pośrednictwem serwisu internetowego:

Limit pojedynczej transakcji Limit wszystkich transakcji w ciągu dnia
1.000 złotych

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.