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

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 następujących elektronicznych kanałów dostępu:
   1) w ramach bankowości elektronicznej - usługi zapewniające dostęp do informacji o produktach i usługach posiadanych w Banku oraz składanie dyspozycji:
      a) bankowość internetowa (serwis internetowy) – 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 Nasz Bank, Novum-13 lub Nasz Bank Junior;
   2) powiadamianie SMS (serwis SMS) – uzyskiwanie informacji związanych z transakcjami na rachunku w formie wiadomości SMS.
2. Wykaz produktów i usług dostępnych za pośrednictwem elektronicznych kanałów dostępu oraz warunki korzystania z usług określa Przewodnik dla klienta publikowany na stronie internetowej Banku; Przewodnik dla klienta stanowi instrukcję użytkowania zawierającą opis poszczególnych elektronicznych kanałów dostępu, wymagania techniczne dla każdego kanału i zasady prawidłowego posługiwania się tymi kanałami przez klienta.

§ 2

1. Elektroniczne kanały dostępu mogą być udostępnione wyłącznie w przypadku posiadania przez klienta rachunku oszczędnościowo-rozliczeniowego lub podstawowego rachunku płatniczego; Bank może udostępnić elektroniczne kanały dostępu dla innych rachunków lub produktów bez wymogu posiadania wyżej wymienionych produktów, o czym poinformuje na stronie internetowej Banku.
2. Użytkownikiem korzystającym z elektronicznych kanałów dostępu może być posiadacz, współposiadacz rachunku oraz pełnomocnik, któremu udzielono pełnomocnictwa stałego.
3. Małoletni korzysta z elektronicznych kanałów dostępu na podstawie zgody przedstawiciela ustawowego, w ramach zawartej z Bankiem umowy.
4. 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; szczegółowe zasady składania oświadczeń woli przez użytkownika oraz Bank dotyczące zawarcia umowy lub zmiany jej warunków za pośrednictwem elektronicznych kanałów dostępu, określone są w §7; informacje o ofercie oraz dostępnych sposobach zawierania umów zawarte są na stronie internetowej Banku oraz w Przewodniku dla klienta.
5. Bank udostępnia Kantor SGB dla użytkownika; zasady świadczenia usługi Kantor SGB w ramach usługi bankowości elektronicznej stanowią załącznik nr 4 do regulaminu.

§ 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 przez użytkownika:
   1) zaleca się korzystanie z zaufanych komputerów 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. 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 do bankowości elektronicznej; szczegółowe informacje dotyczące wszystkich stosowanych przez Bank rodzajów plików *cookies* oraz celu ich wykorzystywania dostępne są na stronie internetowej Banku.

§ 5

1. Użytkownik ma obowiązek korzystać z elektronicznych kanałów dostępu zgodnie z umową, regulaminem i Przewodnikiem dla klienta. Użytkownik ma obowiązek zabezpieczyć otrzymane i indywidualne dane uwierzytelniające przed dostępem osób trzecich i zapewnić ich poufność.
2. Z chwilą otrzymania indywidualnych danych uwierzytelniających, o których mowa w ust. 1, użytkownik podejmuje niezbędne środki służące zapobieżeniu naruszenia indywidualnych danych uwierzytelniających. Ze względów bezpieczeństwa poszczególnych danych nie wolno przechowywać razem ze sobą.
3. Bank zapewnia użytkownikowi należytą ochronę indywidualnych danych uwierzytelniających. Indywidualne dane uwierzytelniające są dostępne wyłącznie dla 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.

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, o których mowa w Rozdziale 4 regulaminu, z uwzględnieniem postanowień § 9-12 niniejszego załącznika oraz sposobu posługiwania się danym elektronicznym kanałem dostępu opisanym w *Przewodniku lub Instrukcji dla klienta*.
2. Bank umożliwia użytkownikowi w elektronicznych kanałach dostępu:
   1) składanie wniosku o wypłatę świadczenia wychowawczego w ramach Programu Rodzina 500+ wraz z załącznikami oraz Dobry start – dostępność usługi uzależniona jest od współpracy z Ministerstwem Rodziny i Polityki Społecznej;
   2) składanie innych wniosków udostępnionych przez Bank oraz zawieranie umów w sposób określony w §7;
   3) składanie innych wniosków udostępnionych przez Bank dotyczących produktów lub usług podmiotów trzecich współpracujących z Bankiem;
   4) wymianę walut w Kantorze SGB użytkownikom, którym Bank udostępnił usługę.
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 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, przy czym wybrane dyspozycje złożone przez małoletniego, który nie ukończył 13 roku życia są realizowane po ich zatwierdzeniu w bankowości mobilnej przez przedstawiciela ustawowego[1].
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 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 niewymagających silnego uwierzytelnienia 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 znajduje się na liście zaufanych odbiorców utworzonej uprzednio przez użytkownika przy zastosowaniu silnego uwierzytelnienia;
   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 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 on-line 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 skontaktowania się z użytkownikiem w celu realizacji zlecenia płatniczego.
7. Dostęp użytkownika do serwisu internetowego następuje poprzez:

[1] Po wdrożeniu funkcjonalności przez Bank.

a. aplikację mobywatel;
b. podanie identyfikatora użytkownika oraz udostępnionych użytkownikowi indywidualnych danych uwierzytelniających, o których mowa w ust. 8.

8. Autoryzacja dyspozycji składanych za pośrednictwem serwisu internetowego odbywa się poprzez użycie następujących indywidualnych danych uwierzytelniających:
   1) aplikacji mobilnej i PINu do aplikacji mobilnej lub za pomocą biometrii; wymogi oraz zasady dotyczące instalacji aplikacji mobilnej na urządzeniu mobilnym i sposób jego aktywacji przez użytkownika opisane są w Instrukcji dla Użytkownika, lub
   2) kodu SMS, z zastrzeżeniem ust. 9,
   3) aplikacji nPodpis wraz z certyfikatem (Athena Cryptocard),
   4) tokena spełniającego kryteria silnego uwierzytelniania,

   chyba, że Bank udostępni inne indywidualne dane uwierzytelniające opisane w Instrukcji dla Użytkownika.
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 kodów SMS. 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 w postaci kodów otrzymywanych poprzez wiadomości SMS.
11. Autoryzacja dokonana przez użytkownika jest równoznaczna z poleceniem Bankowi dokonania określonej czynności i stanowi podstawę jej dokonania.
12. Bank przesyła kody SMS na potrzeby aktywacji aplikacji mobilnej oraz wykorzystywane przy stosowanych metodach uwierzytelnienia na numer telefonu komórkowego, który użytkownik wskazał w umowie, karcie informacyjnej lub pełnomocnictwie.
13. Bank może wprowadzić, wycofać oraz zmienić rodzaj stosowanych indywidualnych danych uwierzytelniających poprzez udostępnienie ich użytkownikowi oraz zawiadomienie użytkownika o dokonanej zmianie; informacja o stosowanych rodzajach 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 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 § 27 ust. 5 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) braku środków pieniężnych dla realizacji dyspozycji lub
   5) innych okoliczności uniemożliwiających jej przyjęcie przez Bank,

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

Rozdział 3. Korzystanie z elektronicznych kanałów dostępu

§ 13

Za pośrednictwem elektronicznych kanałów dostępu 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 rachunków za pośrednictwem elektronicznych kanałów dostępu.

Rozdział 4. Ograniczenia w korzystaniu z elektronicznych kanałów dostępu

§ 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 serwisu internetowego;
   2) złożenia przez użytkownika dyspozycji dezaktywacji środka autoryzacyjnego;
   ~~3)~~ kolejnego trzykrotnego wpisania nieprawidłowego PIN do aplikacji mobilnej lub pięciokrotnego hasła dostępu w serwisie www~~.~~
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 serwisu internetowego lub innych systemów teleinformatycznych związanych z wykonywaniem umowy, o czym Bank z wyprzedzeniem poinformuje klienta na stronie internetowej Banku;
   5) dokonywania czynności mających na celu usunięcie awarii, usterek lub nieprawidłowości działania w serwisie internetowym lub innych systemach teleinformatycznych związanych z wykonywaniem umowy;

6) wymiany stosowanych indywidualnych danych uwierzytelniających, o czym Bank z wyprzedzeniem poinformuje użytkownika pisemnie lub 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 na wniosek złożony przez posiadacza rachunku lub pełnomocnika stałego w sposób określony w ust. 4. W takim przypadku Bank wydaje użytkownikowi nowe indywidualne dane uwierzytelniające lub dokona uchylenia ograniczenia lub blokady przy zachowaniu dotychczasowych danych uwierzytelniających.
4. W przypadku, o którym mowa w ust. 2 pkt 1 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.
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. Blokowanie i zastrzeganie dostępu do serwisu internetowego

§ 15

1. Dostęp do serwisu internetowego oraz możliwość posługiwania się indywidualnymi danymi uwierzytelniającymi może zostać zablokowana 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 możliwość dokonanie transakcji.

§ 16

1. W przypadku utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia indywidualnych danych uwierzytelniających lub nieuprawnionego dostępu do serwisu internetowego jego użytkownik/przedstawiciel ustawowy małoletniego powinien go niezwłocznie telefonicznie zastrzec, podając swoje dane personalne.
2. Zastrzeżenia, o którym mowa w ust. 1, można dokonywać:
   1) osobiście w placówce Banku,
   2) telefonicznie pod numerami telefonów wskazanymi i aktualizowanymi przez Bank w komunikacie zamieszczonym w placówkach Banku lub na stronie internetowej Banku, w zakładce Placówki,
   3) poprzez wysłanie wiadomości SMS na numer telefonu 602279320 o treści:
      a) BI#identyfikator
         jeżeli wiadomość wysyłana jest z numeru telefonu powiązanego z usługą Internet Banking,
      b) BI#identyfikator#Pesel
         w pozostałych przypadkach.

3. Bank ma prawo zmiany numerów telefonów, pod którymi dokonywane są zastrzeżenia i 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 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 lub działający w jego imieniu przedstawiciel ustawowy, może wystąpić z wnioskiem o wydanie nowych 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 do dokonania 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) jeżeli nie posiada dotychczasowego telefonu do autoryzacji, konieczne jest złożenie stosownej dyspozycji w placówce Banku.

§ 17

1. Bank ma prawo do zastrzeżenia indywidualnych danych uwierzytelniających:
   1) w przypadku wygaśnięcia lub rozwiązania umowy;
   2) z uzasadnionych przyczyn związanych z bezpieczeństwem indywidualnych danych uwierzytelniających tzn. powzięciem informacji o wejściu w ich posiadanie osób trzecich;
   3) w związku z podejrzeniem 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 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. Potwierdzanie dostępności środków na rachunku

§ 18

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:
   a) rachunek płatniczy płatnika (użytkownika) jest dostępny on-line w momencie występowania z wnioskiem, oraz
   b) 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
   c) zgoda, o której mowa w pkt b, 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 transakcji oraz limity wszystkich transakcji w ciągu dnia

§ 19

1. Standardowe oraz maksymalne limity pojedynczej transakcji 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	Standardowy limit pojedynczej transakcji	Standardowy limit wszystkich transakcji w ciągu dnia	Maksymalny limit pojedynczej transakcji	Maksymalny limit wszystkich transakcji w ciągu dnia
Złoty polski	2.000	10.000	10.000	50.000
Funt brytyjski	500	2.500	2.500	10.000
Dolar amerykański	500	2.500	2.500	10.000
Euro	500	2.500	2.500	10.000

2. Standardowe limity pojedynczej transakcji oraz limity wszystkich transakcji w ciągu dnia dokonanych za pośrednictwem aplikacji mobilnej Nasz Bank:

Waluta rachunku	Standardowy limit pojedynczej transakcji	Standardowy limit wszystkich transakcji w ciągu dnia	Maksymalny limit pojedynczej transakcji	Maksymalny limit wszystkich transakcji w ciągu dnia
Złoty polski	500	1.000	2.000	4.000
Funt brytyjski	500	1.000	2.000	4.000
Dolar amerykański	500	1.000	2.000	4.000
Euro	500	1.000	2.000	4.000

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

Rozdział 8. Aplikacja mobilna

§ 20

1. Aplikacje mobilne stanowią dodatkowy elektroniczny kanał dostępu, za pośrednictwem którego użytkownik może mieć dostęp do produktów i usług, z których korzysta na podstawie umowy produktowej oraz składać określone dyspozycje do tych rachunków m.in. realizacji przelewu, mobilnej autoryzacji, założenia lokaty, doładowania telefonu itd., których pełna lista znajduje się w Instrukcji dla Użytkownika.
2. Bank udostępnia aplikację mobilną:
   1) na urządzenie mobilne z systemem operacyjnym iOS ze sklepu App Store;
   2) na urządzenie mobilne z systemem operacyjnym Android ze sklepu Google Play.

3. Aktywacji aplikacji można dokonać za pomocą indywidualnych danych uwierzytelniających wykorzystywanych przez użytkownika do logowania w bankowości internetowej.
4. Aktywacja aplikacji wymaga spełnienia łącznie poniższych warunków:
   1) podania przez użytkownika danych do logowania do bankowości internetowej;
   2) udzielenia przez użytkownika zgody na korzystanie z aplikacji;
   3) zaakceptowania przez użytkownika treści regulaminu;
   4) użycia kodu przesłanego za pomocą SMS na numer telefonu komórkowego i zarejestrowanie urządzenia mobilnego jako zaufanego urządzenia mobilnego.
5. Aktywacja aplikacji mobilnej jest równoznaczna z udostępnieniem bankowości internetowej przez bank w ramach zawartej umowy produktowej, z zastrzeżeniem, że bank może udostępnić bankowość internetową bez konieczności aktywacji aplikacji.
6. Użytkownik jest zobowiązany używać aplikacji pochodzącej z wiarygodnego źródła (wyłącznie ze sklepów Google Play oraz App Store).
7. Zaleca się, by użytkownik zapewnił ochronę zaufanego urządzenia mobilnego przy pomocy:
   a. kodu odblokowującego ekran;
   b. programu antywirusowego.
8. Nie zaleca się otwierania na zaufanym urządzeniu mobilnym wiadomości e–mail, załączników do e-mail i linków do stron WWW, pochodzących z nieznanych źródeł i od nieznanych osób.
9. W trakcie korzystania z aplikacji, komunikacja pomiędzy zaufanym urządzeniem mobilnym, a serwerem Banku jest szyfrowana protokołem SSL, z zastosowaniem certyfikatu wystawionego i uwierzytelnionego dla serwera bankowego.
10. Bank określa wymogi bezpieczeństwa, które musi spełniać PIN do aplikacji i prezentuje je w czasie ustalania lub zmiany PIN-u do aplikacji.
11. Użytkownik aplikacji jest zobowiązany do:
    a. ochrony PIN-u do aplikacji oraz zaufanego urządzenia mobilnego przed nieuprawnionym przejęciem lub użyciem przez osoby trzecie;
    b. niezwłocznego zgłoszenia do banku utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia zaufanego urządzenia mobilnego lub PIN-u;
    c. niezwłocznego zgłoszenia do banku nieuprawnionego użycia aplikacji mobilnej przez osoby nieuprawnione;
    d. nieudostępniania zaufanego urządzenia mobilnego osobom nieuprawnionym;
    e. przechowywania PIN-u do aplikacji oraz zaufanego urządzenia mobilnego z zachowaniem należytej staranności.
12. Zgłoszenie utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia zaufanego urządzenia mobilnego lub aplikacji następuje:
    a. w placówce banku;
    b. telefonicznie pod numerem telefonu wskazanym na stronie internetowej banku oraz w komunikatach lub materiałach informacyjnych dostępnych w placówkach banku.
13. Na podstawie zgłoszenia, o którym mowa ust. 11, bank blokuje dostęp do aplikacji, co uniemożliwia posługiwanie się aplikacją na zaufanym urządzeniu mobilnym.
14. Za udostępnienie zaufanego urządzenia mobilnego, udostępnienie aplikacji lub ujawnienie PIN-u do aplikacji osobom trzecim odpowiedzialność ponosi użytkownik aplikacji.
15. Bank jest zobowiązany zablokować dostęp do aplikacji, uniemożliwiając tym samym wykonanie dyspozycji, w jednym z następujących przypadków:
    a. złożenia przez użytkownika dyspozycji zablokowania lub dezaktywacji aplikacji;
    b. 3-krotnego wprowadzenia nieprawidłowego PIN-u do aplikacji.

16. Bank ma prawo częściowo ograniczyć lub zablokować dostęp do aplikacji i/lub czasowo zablokować wykonanie dyspozycji w następujących przypadkach:
    a. uzasadnionych przyczyn związanych z bezpieczeństwem, tj.:
        i. uzyskania informacji w tym podejrzenia, iż dyspozycje w aplikacji składane są przez osoby nieuprawnione,
        ii. zagrożenia przechwycenia danych dostępowych przez złośliwe oprogramowanie,
        iii. wykorzystywania danych dostępowych przez oprogramowanie automatycznie logujące się z dużą częstotliwością,
        iv. wykorzystywania systemów lub rachunków w sposób niezgodny z obowiązującymi przepisami prawa,
        v. wykonywania działań mogących zagrażać bezpieczeństwu systemu i danych w nim przetwarzanych;
    b. podejrzenia nieuprawnionego użycia aplikacji, zaufanego urządzenia mobilnego, indywidualnych danych uwierzytelniających lub umyślnego doprowadzenia do nieautoryzowanej dyspozycji;
    c. powzięcia informacji o zagrożeniu bezpieczeństwa dyspozycji;
    d. dokonywania czynności konserwacyjnych aplikacji lub innych systemów teleinformatycznych, związanych z korzystaniem z aplikacji, o czym bank z wyprzedzeniem poinformuje użytkownika na stronie internetowej banku;

e. dokonywania czynności mających na celu usunięcie awarii, usterek lub nieprawidłowości działania aplikacji lub innych systemów teleinformatycznych związanych z jej obsługą.

§ 21

1. Szczegółowy zakres usług dostępnych w aplikacjach mobilnych określają:
    a. Instrukcja dla Użytkownika po aplikacji Nasz Bank;
    b. Instrukcja dla Użytkownika po aplikacji Novum-13 – Bankowość dla najmłodszych.
    c. Instrukcja dla Użytkownika po aplikacji Nasz Bank Junior – Bankowość dla najmłodszych
2. Dokumenty, o których mowa w ust.1 stanowią instrukcje użytkowania aplikacji mobilnych i zmiany w nich wprowadzone nie wymagają powiadamiania klienta w trybie przewidzianym dla regulaminu; aktualna treść tych dokumentów zamieszczona jest na stronie internetowej Banku.
3. Informacja o możliwości rozszerzenia zakresu usług dostępnych w aplikacjach mobilnych przekazywana jest użytkownikowi w aplikacjach mobilnych, których dotyczą.

Rozdział 9. Inne postanowienia

§ 22

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.