Zasady udostępniania i funkcjonowania elektronicznych kanałów dostępu

§ 1

1. Niniejszy załącznik do „Regulaminu świadczenia usług w zakresie prowadzenia rachunków bankowych dla klientów indywidualnych" określa prawa i obowiązki użytkowników instrumentów płatniczych.

2. Przez określenia użyte w niniejszym załączniku do regulaminu należy rozumieć:

1) **adres elektroniczny** – oznaczenie systemu teleinformatycznego umożliwiającego porozumiewanie się za pomocą środków komunikacji elektronicznej, w szczególności adresu poczty elektronicznej e-mail w sieci internet;

2) **autoryzacja** – zgodę na dokonanie transakcji płatniczej, udzieloną odpowiednio przez posiadacza rachunku, pełnomocnika, posiadacza karty, użytkownika karty lub użytkownika systemu, w sposób określony w regulaminie;

3) **elektroniczny kanał dostępu** – sposób komunikacji posiadacza rachunku z Bankiem lub Banku z posiadaczem na odległość, za pośrednictwem sieci teleinformatycznej lub urządzeń elektronicznych, obejmujący w szczególności: usługi bankowości elektronicznej (serwis internetowy) Internet Banking, powiadamianie SMS (SMS Banking);

4) **indywidualne dane uwierzytelniające** – indywidualne dane zapewniane użytkownikowi przez dostawcę usług płatniczych do celów uwierzytelniania;

5) **przewodnik dla klienta –** dokument określający szczegóły świadczenia usług przez Bank oraz zasady użytkowania systemu (np. Przewodnik po SGB Mobile, Przewodnik użytkownika – aplikacja mobilna Nasz Bank, Przewodnik użytkownika – aplikacja mobilna Nasz Bank Junior.

6) **klucz zabezpieczający U2F / klucz sprzętowy** – Universal 2 Factor, urządzenie zewnętrzne służące do silnego uwierzytelniania wieloskładnikowego przy użyciu pary kluczy – prywatnego i publicznego. Do autoryzacji wymagane jest fizyczne użycie klucza zabezpieczającego U2F.

7) **silne uwierzytelnianie** - uwierzytelnianie zapewniające ochronę poufności danych w oparciu o zastosowanie co najmniej dwóch elementów należących do kategorii:

a) wiedza o czymś, o czym wie wyłącznie użytkownik,

b) posiadanie czegoś, co posiada wyłączenie użytkownik,

c) cechy charakterystyczne użytkownika

będących integralna częścią tego uwierzytelniania oraz niezależnych w taki sposób, że naruszenie jednego z tych elementów nie osłabia wiarygodności pozostałych;

8) **system** – system teleinformatyczny służący Bankowi do przekazywania użytkownikowi systemu informacji związanych z obsługą jego rachunków oraz tworzenia i wymiany elektronicznych komunikatów pozwalających użytkownikowi systemu na przygotowanie dyspozycji oraz przesłanie ich do Banku;

9) **uwierzytelnianie** – procedurę umożliwiającą Bankowi weryfikację tożsamości użytkownika lub ważności stosowania konkretnego instrumentu płatniczego, łącznie ze stosowaniem indywidualnych danych uwierzytelniających;

10) **użytkownik systemu** – odpowiednio posiadacza rachunku lub współposiadacza rachunku, z którym Bank zawarł umowę lub pełnomocnika, który został przez posiadacza rachunku umocowany do dysponowania rachunkiem za pośrednictwem elektronicznych kanałów dostępu i który otrzymał od Banku indywidualne dane uwierzytelniające.

Rozdział 1. Udostępnienie i warunki korzystania z elektronicznych kanałów dostępu

§ 2

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 SGB Mobile, Nasz Bank lub Nasz Bank Junior;
   2) powiadamianie SMS (serwis SMS) – uzyskiwanie informacji związanych z transakcjami na rachunku oraz aktualnym saldzie rachunku w formie wiadomości SMS
   3) innego kanału oferowanego przez Bank, jeżeli umowa umożliwia korzystanie z innego kanału.
      3.1 Bank udostępnia wszystkim użytkownikom bankowości elektronicznej możliwość stosowania klucza zabezpieczającego U2F/klucza sprzętowego jako formy zabezpieczeń bankowości elektronicznej chroniącej przed phishingiem i wyłudzeniami danych do logowania zgodnie z Regulaminem ***korzystania z funkcji dwuetapowego logowania kluczami U2F w Banku Spółdzielczym w Człuchowie.*** Regulamin, o którym mowa w niniejszym punkcie Bank udostępnia na stronie internetowej www.bsczluchow.pl oraz Internet Banking.
      3.2 Metoda zabezpieczeń o której mowa w ust. 3.1 nie jest obligatoryjna dla Użytkowników bankowości elektronicznej, ale zalecana do stosowania.

2. Wykaz produktów i usług dostępnych za pośrednictwem elektronicznych kanałów dostępu oraz warunki korzystania z usług określa przewodnik dla klienta.

3. Informacje dotyczące aktualnej oferty usług dostępnych w aplikacjach mobilnych opisane są w przypadku:
   1) aplikacji mobilnej SGB Mobile w Regulaminie korzystania z aplikacji mobilnej SGB Mobile,
   2) aplikacji mobilnej Nasz Bank w Przewodniku użytkownika;
   3) aplikacji mobilnej Nasz Bank Junior w Przewodniku użytkownika;
   ww. dokumenty zamieszczone są na stronie internetowej Banku.

§ 3

1. Elektroniczne kanały dostępu mogą być udostępnione wyłącznie w przypadku posiadania przez klienta rachunku oszczędnościowo-rozliczeniowego lub podstawowego rachunku płatniczego, chyba, że Regulamin korzystania z aplikacji mobilnej SGB Mobile stanowi inaczej.

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, 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 określa przewodnik dla klienta.

§ 4

1. Użytkownik uzyskuje dostęp do bankowości elektronicznej za pomocą indywidualnych danych uwierzytelniających, z zastrzeżeniem § 10**.**

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 §§ 21-24.

§ 5

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 systemu 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.

§ 6

1. Użytkownik ma obowiązek korzystać z elektronicznych kanałów dostępu zgodnie z umową, regulaminem. Użytkownik ma obowiązek zabezpieczyć otrzymane 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.

§ 7

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

Rozdział 2. Dyspozycje składane za pośrednictwem elektronicznych kanałów dostępu

§ 8

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 indywidualnych danych uwierzytelniających dokonana została poprawna identyfikacja użytkownika składającego oświadczenie woli, z zastosowaniem wymaganych przez Bank metod uwierzytelniania.

§ 9

1. Do dysponowania rachunkami bankowymi 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 §§ 10-13 niniejszego załącznika oraz sposobu posługiwania się danym elektronicznym kanałem dostępu opisanym w przewodniku dla klienta oraz umowie.

2. Zakres operacji udostępnianych użytkownikowi systemu przez Bank w ramach usługi może obejmować:

1) dokonywanie operacji biernych:

a) uzyskiwanie ogólnie dostępnych informacji o usługach bankowych, zasadach bezpiecznego użytkowania karty, systemu itp.;

b) uzyskiwanie informacji o rachunkach bankowych, w tym kredytowych; posiadanych w Banku oraz operacjach dostępnych dla tych rachunków,

c) uzyskiwanie powiadomień SMS o operacjach przeprowadzonych na rachunku oraz o aktualnym saldzie rachunku, jak również uzyskiwanie kodów służących do autoryzacji dyspozycji złożonych za pośrednictwem elektronicznych kanałów dostępu,

d) otrzymywanie zawiadomień o dokonanych przez Bank zmianach w treści umowy, regulaminu lub Taryfy, a także o zmianach wprowadzonych w systemie, mających wpływ na zmianę dotychczasowego trybu dokonywania operacji biernych lub aktywnych;

2) dokonywanie operacji aktywnych:

a) składanie, zmianę dyspozycji płatniczych z rachunków, o których mowa w pkt 1 lit. b, na inne rachunki bankowe w Banku lub w innych bankach w kraju i zagranicą, z wyłączeniem rachunków kredytowych,

b) odwoływanie niewykonanych jeszcze przez Bank dyspozycji płatniczych z odroczonym terminem realizacji,

c) tworzenie, zmianę listy zdefiniowanych odbiorców (baza kontrahentów),

d) składanie, zmianę zleceń stałych,

e) odwoływanie niewykonanych jeszcze przez Bank zleceń stałych,

f) pobieranie wydruku potwierdzenia wykonania operacji,

g) zastrzeganie kart,

h) składanie oświadczeń woli o otwarciu lub zamknięciu rachunku lokaty w ramach umowy;

i) składanie wniosku o wypłatę świadczenia wychowawczego w ramach Programu Rodzina 800+ wraz z załącznikami oraz Dobry start – dostępność usługi uzależniona jest od współpracy z Ministerstwem Rodziny i Polityki Społecznej;

j) składanie innych wniosków udostępnionych przez Bank dotyczących produktów lub usług podmiotów trzecich współpracujących z Bankiem;

k) uwierzytelnianie logowania do Profilu Zaufanego – „***Regulamin świadczenia usług identyfikacji elektronicznej SGB ID dla klientów indywidualnych***”, został opublikowany pod adresem: https://www.sgb.pl/wp-content/uploads/2020/06/Regulamin-swiadczenia-uslug-identyfikacji-elektronicznej-_20200521.pdf,

l) składanie zamówienia na wypłatę środków w bankomacie w ramach sm@rt wypłaty, której limit wynosi 1 000,00 zł zarówno dla transakcji składanej za pośrednictwem elektronicznych kanałów dostępu, jak i w Banku. W przypadku złożenia zamówienia o sm@rt wypłatę w Banku, pracownik jest zobowiązany wydrukować potwierdzenie zamówienia zawierające kod wypłaty z systemu operacyjnego, na którym klient akceptuje regulamin funkcjonowania usługi. Kod wypłaty ważny jest przez 15 minut;

m) zakładanie i administrowanie skarbonkami dzieci w ramach aplikacji mobilnej Nasz Bank Junior;

n) wysłanie prośby o doładowanie telefonu[1]. Zainicjowana przez dziecko transakcja poprzedzona jest wysłaniem do aplikacji rodzica prośby o wygenerowanie i udostępnienie kodu BLIK, a następnie zatwierdzona jest akceptacją rodzica.

o) wysłanie prośby o kod Blik[2].
Aplikacja umożliwia dzieciom przesłanie prośby o doładowanie telefonu na kartę w postaci komunikatu widocznego w bankowości internetowej i aplikacji mobilnej rodzica Nasz Bank.

3) dokonywanie innych czynności z Bankiem, w tym w szczególności:

[1] Dotyczy aplikacji Nasz Bank Junior

[2] Dotyczy aplikacji Nasz Bank Junior

a) dokonywanie zmiany indywidualnych danych uwierzytelniających (np. zmiana hasła dostępu),
b) składanie zamówienia na indywidualne dane uwierzytelniające;
c) zmiana sposobu autoryzacji z mobilnej na hasła SMS w przypadku utraty dostępu do aplikacji mobilnej „Nasz Bank", po udzieleniu odpowiedzi na dodatkowe pytania weryfikacyjne,
d) pobierania plików udostępnionych przez Bank;
e) przesyłanie komunikatów kierowanych do Banku zawierających zapytanie lub reklamację;
f) składanie wniosków o kredyt gotówkowy;
g) składanie wniosków o zmianę limitu pojedynczej transakcji/sumy transakcji dziennych;
h) składanie wniosków o instrument płatniczy;
i) składanie wniosków o zmianę danych osobowych;
j) składanie wniosków o anulowanie przelewu.

3. Aktualny zakres usług dostępnych za pośrednictwem elektronicznych kanałów dostępu określa odpowiednia dla danego kanału przewodnik dla klienta.
4. Bank świadczy usługę oferowaną przez integratorów płatności internetowych, którzy inicjują płatności w formie przelewów typu pay by link we współpracy z Bankiem.
5. Bank realizuje zlecenie płatnicze inicjowane przez innych dostawców świadczących usługę inicjowania transakcji płatniczej zgodnie z zapisami przepisu nr 1.
6. 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.
7. Zgody na wykonanie transakcji płatniczej użytkownik może udzielić również za pośrednictwem dostawcy świadczącego usługę inicjowania transakcji płatniczych.
8. 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.

§ 10

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.[3]
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] Po wdrożeniu funkcjonalności przez Bank.

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 on-line 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 systemu, 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 on-line oraz odkąd ostatni raz zastosowano silne uwierzytelnienie użytkownika.

6. Bank zastrzega sobie prawo skontaktowania się z użytkownikiem w celu realizacji zlecenia płatniczego.

6.1. Zlecenia płatnicze zewnętrzne w kwocie ≥ 100 000,00 zł przesłane za pośrednictwem elektronicznych kanałów dostępu (Internet Banking), podlegają autoryzacji w systemie informatycznym. Autoryzacja polega na telefonicznym potwierdzeniu danych przez klienta, który składał dyspozycję wykonania zlecenia ze swojego rachunku. Akceptacja dokumentu przez osobę autoryzującą oznacza, że klient potwierdził złożenie danego zlecenia.

6.2. Rozmowa o której mowa w ust. 6.1 jest nagrywana, o czym Bank jest zobowiązany poinformować klienta przed rozpoczęciem potwierdzenia i akceptacji wykonywanego przez niego polecenia przelewu.

6.3. Czynność, o której mowa w ust. 6.2 jest możliwa do zrealizowania wyłącznie, gdy klient wyraził na to zgodę we wniosku o Elektroniczne kanały dostępu.

6.4. Telefonicznej autoryzacji zrealizowanej przez klienta transakcji, o której mowa w ust. 6.1, pracownik Baku dokonuje przed godzinami granicznymi ustalonymi dla zleceń płatniczych zawartych w Regulaminie świadczenia usług w zakresie prowadzenia rachunków bankowych dla klientów indywidualnych w Banku Spółdzielczym w Człuchowie.

6.5. Za czynność, o której mowa w ust. 6.1 Bank nie pobiera opłat.

7. Dostęp i autoryzacja dyspozycji składanych za pośrednictwem serwisu internetowego odbywa się, po zalogowaniu do serwisu internetowego, poprzez użycie następujących indywidualnych danych uwierzytelniających:

1) identyfikatora, hasła stałego lub

2) kodu SMS wraz z kodem uwierzytelnienia, z zastrzeżeniem § 19 ust.1 lub,

3) e-PIN-ów przypisanych do aplikacji mobilnych oferowanych przez Bank, w przypadku operacji zatwierdzanej w aplikacji;

chyba, że Bank udostępni inne indywidualne dane uwierzytelniające, opisane w przewodniku dla klienta.

8. Autoryzacja dyspozycji składanych za pośrednictwem elektronicznego kanału dostępu, o którym mowa w § 1 ust. 1 pkt 3, odbywa się poprzez podanie, za pośrednictwem telefonu z funkcją wybierania tonowego, identyfikatora oraz hasła dostępu.

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 telefon 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 oraz zawiadomienie użytkownika systemu o dokonanej zmianie; informacja o stosowanych rodzajach indywidualnych danych uwierzytelniających jest zamieszczona w przewodniku dla klienta oraz na stronie internetowej Banku.

§ 11

Jeżeli z postanowień umowy lub 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.

§ 12

1. Realizacja dyspozycji składanych za pośrednictwem bankowości elektronicznej odbywa się drogą elektroniczną, 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 § 34 ust. 6-9 regulaminu.

§ 13

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

Rozdział 3. Korzystanie z elektronicznych kanałów dostępu

§ 14

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

§ 15

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) zastrzeżenia przez użytkownika;
   3) powzięcia podejrzenia, iż osoba trzecia mogła uzyskać dostęp do indywidualnych danych uwierzytelniających w następstwie czego może dojść do logowania z adresów IP z czarnej listy lub realizacji przelewów na rachunki z czarnej listy, zgodnie z obowiązującymi w Banku procedurami;
   4) kolejnego, trzykrotnego wpisania nieprawidłowego hasła dostępu do systemu.

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. 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) w związku z wystąpieniem restrykcji geolokalizacyjnych lub realizacją przelewów na rachunki z szarej listy, zgodnie z obowiązującymi w Banku regulacjami;
   4) korzystania przez użytkownika z serwisu internetowego niezgodnie z zasadami bezpieczeństwa określonymi w niniejszym załączniku lub w sposób zagrażający bezpieczeństwu korzystania z serwisu internetowego;
   5) dokonywania czynności konserwacyjnych serwisu internetowego lub innych systemów teleinformatycznych związanych z wykonywaniem umowy, o czym Bank z wyprzedzeniem poinformuje klienta na stronie internetowej Banku;
   6) dokonywania czynności mających na celu usunięcie awarii, usterek lub nieprawidłowości działania serwisu internetowego lub innych systemów teleinformatycznych związanych z wykonywaniem umowy;
   7) 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 przypadkach, o których 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, pracownik Banku kontaktuje się telefonicznie lub pisemnie z klientem i po potwierdzeniu przez klienta złożonej dyspozycji dokonuje jej odblokowania.

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 5 i 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.

Rozdział 5. Blokowanie i zastrzeganie dostępu do serwisu internetowego

§ 16

1. Dostęp do serwisu internetowego oraz możliwość posługiwania się indywidualnymi danymi uwierzytelniającymi może zostać zablokowana przez:
   1) Bank – zgodnie z postanowieniami § 18;
   2) Użytkownika;
   3) Przedstawiciela ustawowego małoletniego.
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/przedstawiciel ustawowy małoletniego powinien go niezwłocznie telefonicznie zastrzec, podając swoje dane personalne.
2. Zastrzeżenia, o którym mowa w ust. 1, można dokonywać w placówce Banku lub pod numerami telefonów wskazanymi i aktualizowanymi przez Bank w komunikacie zamieszczonym w placówkach Banku oraz na stronie internetowej Banku, a także za pośrednictwem udostępnionych przez Bank elektronicznych kanałów dostępu.
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.

§ 18

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.
1. Z zastrzeżeniem ust. 3, Bank informuje posiadacza rachunku o zamiarze zastrzeżenia indywidualnych danych uwierzytelniających w przypadkach określonych w ust. 1 pkt 2-3, przed ich zastrzeżeniem, a jeżeli nie jest to możliwe – niezwłocznie po jego zastrzeżeniu, telefonicznie.

2. Bank nie przekazuje informacji o zastrzeżeniu, jeżeli przekazanie tej informacji byłoby nieuzasadnione ze względów bezpieczeństwa lub zabronione na mocy odrębnych przepisów.

Rozdział 6. Urządzenie zaufane

§ 19

1. Użytkownik systemu bankowości internetowej może zdefiniować urządzenie, z którego następuje logowanie do bankowości internetowej jako urządzenie zaufane. Kolejne logowania z tego urządzenia nie będą wymagały dodatkowego uwierzytelnienia użytkownika za pomocą kodów SMS. Urządzeniem zaufanym może być prywatny komputer, smartfon lub tablet, z którego korzysta wyłącznie użytkownik. Bank podczas procesu logowania weryfikuje określone cechy tego urządzenia.

2. Dodanie urządzenia przez użytkownika systemu wymaga:

1) autoryzacji za pośrednictwem udostępnionej użytkownikowi systemu metody autoryzacji, o której mowa w § 10 ust. 7,

2) akceptacji oświadczenia, iż klient jest jedynym użytkownikiem urządzenia i wyraża zgodę, na dodanie urządzenia jako zaufanego na potrzeby silnego uwierzytelnienia podczas logowania do systemu bankowości elektronicznej,

3) akceptacji niniejszych zasad.

3. Użytkownik w dowolnym momencie ma możliwość poprzez bankowość internetową usunięcia swojego urządzenia zaufanego, a każde kolejne logowanie do bankowości internetowej będzie wymagało dodatkowego potwierdzenia w postaci kodów otrzymywanych poprzez wiadomości SMS.

Rozdział 7. Udostępnianie informacji na potrzeby świadczenia usług inicjowania transakcji płatniczych i usług dostępu do informacji o rachunku. Potwierdzenie dostępności środków na rachunku

§ 20

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.

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 systemu oraz

3) zgoda, o której mowa w lit. 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 Banku 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 8. Standardowe limity pojedynczej operacji oraz limity wszystkich operacji w ciągu dnia dokonywanych za pośrednictwem serwisu internetowego

§ 21

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

Rodzaj limitu	Standardowy limit obowiązujący w Banku	Indywidualny limit ustalony na wniosek posiadacza rachunku[4]
Limit pojedynczej transakcji	**3 000,00 zł**	**do 30 000,00 zł**
Limit sumy transakcji dziennych	**20 000,00 zł**	**do 60 000,00 zł**

2. Standardowe limity pojedynczej operacji oraz limity wszystkich operacji w ciągu dnia dokonywanych za pośrednictwem serwisu internetowego dla rachunków w walutach wymienialnych:

[4] Przelewy, których wartość przekracza limit indywidualny, można składać w placówkach Banku w tradycyjnej formie (papierowej).

Rodzaj limitu	Standardowy limit obowiązujący w Banku	Indywidualny limit ustalony na wniosek posiadacza rachunku
Limit pojedynczej transakcji	650 EUR	do 6500 EUR
Limit sumy transakcji dziennych	4300 EUR	do 13 000 EUR

3. Z zastrzeżeniem ust. 3 użytkownik, może wnioskować o indywidualne ustalenie limitów, o których mowa w ust. 1 i 2.
4. O wysokości limitów ostatecznie decyduje Bank.

§ 22

Standardowe limity pojedynczej operacji oraz limity wszystkich operacji w ciągu dnia dokonywanych za zakupy w sklepach internetowych.

Rodzaj limitu	Standardowy limit obowiązujący w Banku
Limit dla pojedynczej transakcji	**3 000,00 zł**
Limit sum transakcji dziennych	**6 000,00 zł**

§ 23

Standardowe limity pojedynczej operacji oraz limity wszystkich operacji w ciągu dnia dokonywanych za pośrednictwem aplikacji mobilnej Nasz Bank.

Rodzaj limitu	Standardowy limit obowiązujący w Banku
Limit pojedynczej transakcji	**300,00 zł**
Limit sum transakcji dziennych	**1 000,00 zł**

§ 24

Standardowe limity pojedynczej operacji oraz limity wszystkich operacji w ciągu dnia dokonywanych za pośrednictwem interfejsu API (PSD2).

Rodzaj limitu	Standardowy limit obowiązujący w Banku

Limit pojedynczej transakcji	**300,00 zł**
Limit sum transakcji dziennych	**1 000,00 zł**

§ 25

Standardowy globalny dzienny limit dla transakcji gotówkowych, bezgotówkowych oraz internetowych, realizowanych za pośrednictwem usługi BLIK.

Rodzaj limitu	Standardowy limit obowiązujący w Banku
Globalny dzienny limit dla transakcji gotówkowych, bezgotówkowych oraz internetowych	**5 000,00 zł**

Rozdział 9. Inne postanowienia

§ 26

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.

Rozdział 10. Usługa biometryczna

§ 27

1. Usługa biometryczna polega na identyfikacji użytkownika na podstawie danych biometrycznych tj. elektronicznego zapisu odwzorowania sieci naczyń krwionośnych dłoni.
2. Udostępnienie usługi biometrycznej następuje na podstawie wniosku użytkownika.
3. Usługa biometryczna jest aktywowana z chwilą wprowadzenia danych użytkownika do systemu informatycznego.
4. Dane, o których mowa w ust. 1, są przetwarzane przez Bank w systemie informatycznym wyłącznie w celu identyfikacji użytkownika oraz autoryzacji transakcji płatniczych użytkownika z wykorzystaniem czytnika biometrycznego.
5. Dane biometryczne są pobierane przez Bank za pośrednictwem urządzeń spełniających normy bezpieczeństwa oraz zapewniających wierność i dokładność zapisu.
6. Bank nie ponosi odpowiedzialności za niewykonanie identyfikacji lub autoryzacji biometrycznej spowodowane siłą wyższą lub następstwem wykonywania obowiązków wynikających z przepisów prawa.