

Wyciąg z „Regulaminu świadczenia usług w zakresie prowadzenia rachunków bankowych dla klientów indywidualnych w Banku Spółdzielczym Ziemi Łowickiej w Łowiczu”

Wyciąg z „Regulaminu świadczenia usług w zakresie prowadzenia rachunków bankowych dla klientów instytucjonalnych w Banku Spółdzielczym Ziemi Łowickiej w Łowiczu”

(obowiązuje od 16.06.2025 r.)



Załącznik nr 3

do „Regulaminu świadczenia usług w zakresie prowadzenia rachunków bankowych dla klientów **indywidualnych** w Banku Spółdzielczym Ziemi Łowickiej w Łowiczu”

Zasady udostępniania i funkcjonowania elektronicznych kanałów dostępu

Spis treści

Rozdział 1. Udostępnienie i warunki korzystania z elektronicznych kanałów dostępu	1
Rozdział 2. Dyspozycje składane za pośrednictwem elektronicznych kanałów dostępu	2
A. Dyspozycje ogólne	2
B. Autowypłata	4
Rozdział 3. Korzystanie z elektronicznych kanałów dostępu	4
Rozdział 4. Ograniczenia w korzystaniu z elektronicznych kanałów dostępu	4
Rozdział 5. Blokowanie i zastrzeganie dostępu do elektronicznych kanałów dostępu	5
Rozdział 6. Udostępnianie informacji na potrzeby świadczenia usług inicjowania transakcji płatniczych i usług dostępu do informacji o rachunku	5
Potwierdzanie dostępności środków na rachunku	5
Rozdział 7. Aplikacja mobilna Nasz Bank oraz Nasz Bank Junior	5
A. Korzystanie z aplikacji mobilnej	5
B. Zasady bezpieczeństwa	6
C. Ograniczenia w korzystaniu z aplikacji mobilnej	7
D. BLIK w aplikacji mobilnej	7
E. Realizacja transakcji dokonywanych w usłudze BLIK	8
F. BLIK w aplikacji Nasz Bank Junior	9
G. Usługa smartKARTA w aplikacji mobilnej	9
H. Realizacja transakcji dokonywanych w usłudze smartKARTA	9
I. Funkcjonalności dostępne w aplikacji mobilnej Nasz Bank i Nasz Bank Junior	10
Rozdział 8. Standardowe maksymalne limity pojedynczej transakcji oraz limity wszystkich transakcji w ciągu dnia	11
Rozdział 9. Inne postanowienia	12

Rozdział 1. Udostępnienie i warunki korzystania z elektronicznych kanałów dostępu

§ 1

- Bank może świadczyć użytkownikom usługi w zakresie obsługi produktów i usług za pośrednictwem następujących elektronicznych kanałów dostępu:
 - bankowość internetowa w następujących wariantach:
 - serwis internetowy – dostęp do bankowości internetowej poprzez sieć internet (kanał www),
 - interfejs mobilny¹ – dostęp do bankowości internetowej poprzez sieć internet (kanał www) na urządzeniu mobilnym (smartfon, tablet),
 - aplikacja mobilna² – dostęp do bankowości internetowej przy pomocy aplikacji mobilnej SGB Mobile lub aplikacji mobilnej Nasz Bank pobranej na urządzeniu mobilnym; dla osób małoletnich dostępna jest aplikacja mobilna Nasz Bank Junior;
 - usługa SMS Banking – uzyskiwanie informacji związanych z transakcjami na rachunku w formie wiadomości SMS; wiadomości w usłudze SMS Banking wysyłane są codziennie w godz. 6:00-22:00.
- Informacje o produktach i usługach udostępnionych za pośrednictwem elektronicznych kanałów dostępu znajdują się na stronie internetowej Banku.
- Warunki korzystania z usług bankowości internetowej w ramach serwisu internetowego określają *Przewodniki dla klientów*.
- Przewodniki, o których mowa ust. 3, zawierają opisy poszczególnych elektronicznych kanałów dostępu, wymagania techniczne dla każdego kanału i zasady prawidłowego posługiwania się tymi kanałami przez klienta. Regulacje te są udostępnione na stronie internetowej Banku oraz wydawane na życzenie klienta przy zawieraniu umowy.
- Kanał, o którym mowa w ust. 1 pkt 1, jest dostępny w dwóch wariantach:
 - wariant I – z jednoosobową autoryzacją dyspozycji (IB – Internet Banking);
 - wariant II – z jedno lub wieloosobową autoryzacją dyspozycji (IBF – Internet Banking dla Firm) – dedykowany dla rady rodziców, SKO, KZP.
- Użytkownik systemu może korzystać z dostępu do bankowości internetowej za pomocą kanału www, interfejsu mobilnego lub aplikacji mobilnej na podstawie tego samego ID wydanego w Banku.
- Informacje dotyczące aktualnej oferty usług dostępnych w aplikacji mobilnej:
 - SGB Mobile opisane są w Regulaminie korzystania z aplikacji mobilnej SGB Mobile, zamieszczonym na stronie internetowej Banku;
 - Nasz Bank oraz Nasz Bank Junior wyszczególnione są w niniejszym załączniku do regulaminu oraz w *Przewodnikach po tych aplikacjach*.

§ 2

- Elektroniczne kanały dostępu mogą być udostępnione w przypadku posiadania przez klienta rachunku:
 - oszczędnościowego,
 - oszczędnościowo-rozliczeniowego, w tym podstawowego rachunku płatniczego,
 - oszczędnościowego w walucie w walucie wymiennej – warunkiem udostępnienia elektronicznych kanałów dostępu jest posiadanie rachunku oszczędnościowo-rozliczeniowego w walucie PLN, z którego będą pobierane prowizje i opłaty.

¹ Nie dotyczy IBF.

² W przypadku IBF funkcjonalności dostępne w aplikacji mobilnej Nasz Bank zostały wskazane w § 32.

2. Lokaty, kredyty oraz pozostałe rachunki ROR, oszczędnościowe również mogą zostać udostępnione w elektronicznych kanałach dostępu na życzenie klienta, o ile wcześniej uruchomiono bankowość internetową. Szczegółowy zakres funkcjonalności lokat i kredytów w elektronicznych kanałach dostępu został opisany w *Przewodnikach dla klientów*.
3. Użytkownikami korzystającym z elektronicznych kanałów dostępu może być posiadacz, współposiadacz rachunku, osoba reprezentująca posiadacza rachunku oraz pełnomocnik któremu udzielono odpowiedniego pełnomocnictwa.
4. Młodzież korzysta z elektronicznych kanałów dostępu na podstawie zgody przedstawiciela ustawowego, w ramach zawartej z Bankiem umowy.
5. Użytkownik może wnioskować o udostępnienie kolejnych produktów i usług oraz zawierać umowy za pośrednictwem elektronicznych kanałów dostępu, o ile taki sposób zawierania umów został udostępniony przez Bank; informacje o aktualnej ofercie znajdują się na stronie internetowej Banku, natomiast informacje o dostępnych sposobach zawierania umów określa regulamin.
6. Użytkownik w ramach podpisanej umowy w placówce Banku może otworzyć rachunek oszczędnościowy w walucie PLN i/lub w walucie wymiennej, o ile taka funkcjonalność została udostępniona przez Bank.
7. Bank udostępnia Kantor SGB użytkownikom zgodnie z zasadami świadczenia usługi Kantor SGB w ramach usługi bankowości elektronicznej stanowiących załącznik nr 4 do regulaminu.

§ 3

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 dziennych limitów transakcji.

§ 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 *Przewodnikach dla klienta*.
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 internetowej; 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 oraz *Przewodnikami dla klientów*. Użytkownik ma obowiązek zabezpieczyć otrzymane indywidualne dane uwierzytelniające przed dostępem osób trzecich i zapewnić ich poufność.
2. Z chwilą otrzymania indywidualnych danych uwierzytelniających, użytkownik podejmuje niezbędne środki służące zapobieganiu naruszenia indywidualnych danych uwierzytelniających. Ze względu na bezpieczeństwo 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

1. Bank, w przypadku wyrażenia zgody przez klienta, umożliwia skorzystanie z metody Device Fingerprinting (DFP)³, która identyfikuje użytkownika po urządzeniu, z którego się loguje. Urządzenie zostaje oznaczone jako zaufane, dzięki czemu logując się z tego urządzenia klient nie musi stosować metod silnego uwierzytelnienia.
2. Klient powinien być jedynym użytkownikiem urządzenia, które oznaczane jest jako zaufane.
3. Szczegółowe informacje odnośnie metody DFP zostały określone w *Przewodniku dla klienta*.

§ 7

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

Rozdział 2. Dyspozycje składane za pośrednictwem elektronicznych kanałów dostępu

A. Dyspozycje ogólne

§ 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 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 sposobów posługiwania się danym elektronicznym kanałem dostępu opisanych w *Przewodnikach dla klientów*.
2. Bank umożliwia w elektronicznych kanałach dostępu:
 - 1) składanie wniosku o wypłatę świadczenia wychowawczego – dostępność usługi uzależniona jest od współpracy z Ministerstwem Rodziny i Polityki Społecznej;
 - 2) składanie wniosku o terminal POS⁴;
 - 3) wymianę walut w Kantorze SGB użytkownikom, którzy spełnili warunki udostępniania usługi;
 - 4) składanie innych wniosków udostępnionych przez Bank dotyczących produktów lub usług podmiotów trzecich współpracujących z Bankiem.
3. Bank świadczy usługę oferowaną przez integratorów płatności internetowych, którzy inicjują płatności w formie przelewów typu pay by link we współpracy z Bankiem, przy czym:
 - 1) integratorem płatności internetowych jest podmiot świadczący usługi sklepom internetowym lub innym podmiotom prowadzącym sprzedaż towarów lub usług, polegające na udostępnieniu im możliwości przyjmowania płatności od ich klientów za pomocą przelewów typu pay by link,
 - 2) przelew typu pay by link jest realizowany przez klienta dokonującego zapłaty za zakupy w sklepach internetowych lub u innych podmiotów prowadzących sprzedaż towarów lub usług za pośrednictwem integratorów płatności internetowych.
4. Zgody na wykonanie transakcji płatniczej użytkownik może udzielić również za pośrednictwem dostawcy świadczącego usługę inicjowania transakcji płatniczej.
5. W przypadku inicjowania transakcji przez dostawcę świadczącego usługę inicjowania transakcji lub przez odbiorcę lub za jego pośrednictwem, użytkownik nie może odwołać zlecenia płatniczego po udzieleniu dostawcy świadczącemu usługę inicjowania transakcji zgody na zainicjowanie transakcji albo po udzieleniu odbiorcy zgody na wykonanie transakcji.

³ Nie dotyczy IBF.

⁴ Dla usługi IBF opcja dostępna po wdrożeniu funkcjonalności przez Bank.

1. Wszelkie dyspozycje i zlecenia płatnicze w bankowości internetowej, 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 w bankowości mobilnej po ich zatwierdzeniu przez przedstawiciela ustawowego.
2. Po złożeniu dyspozycji lub zlecenia płatniczego w bankowości internetowej, użytkownik dokonuje ich autoryzacji przy użyciu indywidualnych danych uwierzytelniających, z zastosowaniem wymaganych przez Bank metod uwierzytelniania.
3. Autoryzacja dokonana przez użytkownika jest równoznaczna z poleceniem Bankowi dokonania określonej czynności i stanowi podstawę jej dokonania.
4. Bank zastrzega sobie prawo skontaktowania się z użytkownikiem w celu realizacji zlecenia płatniczego.
5. 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 nie wymagających silnego uwierzytelnienia wskazanych w ust. 6.
6. 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. 7;
 - 2) inicjowania transakcji, której odbiorca znajduje się na liście zaufanych odbiorców utworzonej uprzednio przez użytkownika przy zastosowaniu silnego uwierzytelniania;
 - 3) inicjowania kolejnych transakcji należących do serii transakcji cyklicznych, opiewających na tę samą kwotę na rzecz tego samego odbiorcy pod warunkiem, że utworzenie, zmiana lub zainicjowanie pierwszej transakcji cyklicznej odbyło się przy zastosowaniu silnego uwierzytelniania;
 - 4) jeżeli użytkownik inicjuje transakcję płatniczą w sytuacji, gdy płatnik i odbiorca są tą samą osobą fizyczną lub prawną i oba rachunki płatnicze są prowadzone przez Bank;
 - 5) inicjowania przez użytkownika transakcji płatniczej, którą Bank uzna za charakteryzującą się niskim poziomem ryzyka zgodnie z mechanizmem monitorowania transakcji Banku.
7. Bank stosuje silne uwierzytelnianie użytkownika, jeżeli spełniony jest którykolwiek z następujących warunków:
 - 1) użytkownik uzyskuje dostęp do informacji określonych w ust. 6 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. 6 pkt 1 lit. b w trybie online oraz odkąd ostatni raz zastosowano silne uwierzytelnianie użytkownika.
8. Dostęp użytkownika do bankowości internetowej następuje poprzez podanie identyfikatora użytkownika oraz udostępnionych użytkownikowi indywidualnych danych uwierzytelniających, o których mowa w ust. 9.
9. Dostęp i autoryzacja dyspozycji składanych za pośrednictwem bankowości internetowej odbywa się poprzez użycie następujących indywidualnych danych uwierzytelniających:
 - 1) dla wariantu I, o którym mowa w § 1 ust. 5 pkt 1:
 - a) identyfikatora ID (loginu);
 - b) hasła stałego;
 - c) hasła SMS;
 - d) mObywatela⁵;
 - e) klucza bezpieczeństwa U2F;
 - f) kodu uwierzytelniającego;
 - g) aplikacji mobilnej Nasz Bank lub aplikacji mobilnej SGB Mobile i hasła do tych aplikacji (szczegóły dotyczące użytkowania aplikacji opisane są w *Przewodnikach dla klientów po tych aplikacjach*);
 - 2) dla wariantu II, o którym mowa w § 1 ust. 5 pkt 2:
 - a) identyfikatora ID (loginu);
 - b) hasła stałego;
 - c) hasła SMS;
 - d) mObywatela⁵;
 - e) klucza bezpieczeństwa U2F;
 - f) kodu uwierzytelniającego;
 - g) tokena Athena wraz z aplikacją nPodpis (wymogi dotyczące instalacji aplikacji nPodpis na komputerze klienta opisane są w instrukcji użytkownika *Aplikacja nPodpis do obsługi certyfikatu*);
 - h) hasła do tokena Vasco DIGIPASS GO3 i aktualnego wskazania tokena – dotyczy pasywnego użytkownika systemu;
 - i) aplikacji mobilnej Nasz Bank i zatwierdzenie transakcji w tej aplikacji (wymogi dotyczące instalacji aplikacji na urządzeniu mobilnym opisane są w instrukcji użytkownika *Aplikacja mobilna Nasz Bank*),
 chyba że Bank udostępni inne indywidualne dane uwierzytelniające, opisane w *Przewodnikach dla klientów*.
10. Hasła stałe, o którym mowa w ust. 9, jest nadawane przez użytkownika, podczas procesu pierwszego logowania do bankowości internetowej, po przekazaniu przez Bank hasła tymczasowego. Bank określa w *Przewodnikach dla klientów* zasady tworzenia hasła stałego (składniki hasła stałego).
11. Bank umożliwia logowanie do systemu bankowości internetowej za pomocą aplikacji mObywatel⁵ lub klucza bezpieczeństwa U2F. Sposób logowania tymi metodami oraz sposób dodawania klucza został opisany w *Przewodnikach dla klientów*.
12. Użytkownik może modyfikować listę aktywowanych kluczy bezpieczeństwa U2F poprzez dodawanie lub usuwanie poszczególnych kluczy z listy kluczy zabezpieczeń dostępnej w bankowości internetowej.
13. 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. Urządzeniem zaufanym może być np. prywatny komputer, smartfon lub tablet, z których korzysta wyłącznie użytkownik. Bank podczas procesu logowania weryfikuje określone cechy tego urządzenia.
14. Użytkownik w dowolnym momencie ma możliwość poprzez bankowość internetową usunięcia swojego urządzenia zaufanego, wówczas każde kolejne logowanie do bankowości internetowej będzie wymagało dodatkowego potwierdzenia w aplikacji mobilnej (autoryzacja mobilna) lub w postaci kodów otrzymywanych poprzez wiadomości SMS.
15. Użytkownik ma możliwość samodzielnego ustanowienia nowego hasła do serwisu internetowego, np. w przypadku zapomnienia dotychczasowego hasła. Zmiana hasła możliwa jest podczas logowania do bankowości internetowej. Wybór tej opcji skutkuje koniecznością wpisania identyfikatora ID, a następnie numeru telefonu. Po poprawnym wprowadzeniu danych zostanie wysłany e-mail zawierający kod do wpisania na stronie, po wprowadzeniu którego zostaną wyświetlone dodatkowe pytania weryfikujące. Poprawna weryfikacja odpowiedzi spowoduje wysłanie wiadomości SMS zawierającej nowe hasło. Logowanie z jego użyciem wymusi zmianę hasła. Numer telefonu oraz adres e-mail muszą być zgodne z danymi podanymi w Banku.
16. 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 *Przewodnikach dla klientów*.

⁵ Funkcjonalność dostępna po wdrożeniu przez Bank.

17. W przypadku autoryzacji hasłami SMS Bank przesyła kody autoryzacyjne (hasła SMS) wykorzystywane przy stosowanych metodach uwierzytelnienia na numer telefonu komórkowego, który użytkownik wskazał w Banku.

§ 11

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

§ 12

1. Realizacja dyspozycji składanych za pośrednictwem bankowości internetowej 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 § 28 ust. 5 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 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.

B. Autowypłata

§ 13a

1. Bank udostępnia w Internet Banking dla Firm usługę autowypłaty, która polega na przygotowaniu wypłaty do realizacji w kasie w placówce Banku dla dowolnej osoby fizycznej, podając:
 - 1) imię i nazwisko,
 - 2) PESEL,
 - 3) numer dokumentu tożsamości,
 - 4) adres.
2. Wypłata w usłudze autowypłaty odbywa się w kasie Banku na podstawie ważnego dokumentu tożsamości w ściśle określonej kwocie oraz w przedziale czasowym ustalonym przez użytkownika IBF.
3. Zlecenia w usłudze autowypłaty wymagają autoryzacji zgodnie z wydanymi indywidualnymi danymi uwierzytelniającymi i liczbą wymaganych podpisów.
4. Osoba fizyczna, o której mowa w ust. 1, dokonuje wypłaty w kasie Banku na podstawie ważnego dokumentu tożsamości, który został podany przez użytkownika IBF.
5. Szczegóły dotyczące usługi autowypłaty opisuje *Przewodnik dla klienta*.

Rozdział 3. Korzystanie z elektronicznych kanałów dostępu

§ 14

1. Bank zapewnia posiadaczowi dostęp do elektronicznych kanałów dostępu 7 dni w tygodniu, 24 godziny na dobę, z zastrzeżeniem ograniczeń wskazanych w § 15.
2. 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 zawniósł o ograniczony dostęp do rachunków za pośrednictwem elektronicznych kanałów dostępu. Bank może automatycznie udostępnić posiadaczowi rachunku i/lub pełnomocnikowi nowo otwarte rachunki ROR, rachunki lokat oraz rachunki kredytów bez konieczności składania wniosku.

Rozdział 4. Ograniczenia w korzystaniu z elektronicznych kanałów dostępu

§ 15

1. Bank jest zobowiązany zablokować dostęp do bankowości internetowej, uniemożliwiając tym samym wykonanie transakcji, w jednym z następujących przypadków:
 - 1) złożenia przez użytkownika dyspozycji zablokowania dostępu do bankowości internetowej;
 - 2) kolejnego trzykrotnego wpisania nieprawidłowego hasła dostępu.
2. Bank ma prawo częściowo ograniczyć lub zablokować dostęp do bankowości internetowej 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;
 - 7) uzasadnionego podejrzenia, iż transakcje na rachunku użytkownika mają związek z popełnieniem przestępstwa związanego z praniem pieniędzy lub finansowaniem terroryzmu;
 - 8) gdy na rachunku klienta wystąpi zamrożenie wartości majątkowych lub, gdy wobec klienta należy stosować sankcje międzynarodowe lub embarga;
 - 9) braku możliwości zastosowania środków bezpieczeństwa finansowego, w tym brak aktualnego dokumentu tożsamości klienta lub osób upoważnionych do działania w jego imieniu.
3. Bank może uchylić ograniczenie albo blokadę dostępu do bankowości internetowej w przypadku, o którym mowa w ust. 2 pkt 1, na wniosek złożony przez posiadacza rachunku lub pełnomocnika, Bank wyda użytkownikowi nowe indywidualne dane uwierzytelniające lub dokona uchylecia ograniczenia lub blokady przy zachowaniu dotychczasowych danych uwierzytelniających.
4. W przypadkach, o których mowa w ust. 2 pkt 2-6, ograniczenie lub blokada dostępu do bankowości internetowej 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 bankowości internetowej następuje na podstawie telefonicznej lub złożonej w Banku dyspozycji klienta;
 - 2) czasowej blokady dyspozycji następuje po telefonicznym lub pisemnym kontakcie pracownika Banku z klientem i po potwierdzeniu przez klienta złożonej dyspozycji.

6. Z zastrzeżeniem ust. 7, 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.
7. Bank nie przekazuje informacji o zablokowaniu, jeżeli przekazanie tej informacji byłoby nieuzasadnione ze względów bezpieczeństwa lub zabronione na mocy odrębnych przepisów.
8. 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 elektronicznych kanałów dostępu

§ 16

1. Dostęp do bankowości internetowej oraz możliwość posługiwania się indywidualnymi danymi uwierzytelniającymi mogą zostać zablokowane przez:
 - 1) Bank – zgodnie z postanowieniami § 18;
 - 2) użytkownika;
 - 3) przedstawiciela ustawowego małoletniego.
2. Na wniosek posiadacza rachunku Bank może zablokować dostęp do bankowości internetowej uniemożliwiając jednocześnie możliwość dokonania transakcji.

§ 17

1. W przypadku utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia indywidualnych danych uwierzytelniających lub nieuprawnionego dostępu do bankowości internetowej jego użytkownik/przedstawiciel ustawowy małoletniego powinien go niezwłocznie telefonicznie zastrzec, podając swoje dane personalne.
2. Zastrzeżenia, o którym mowa w ust. 1, można dokonywać osobiście w placówce Banku lub pod numerami telefonów wskazanymi i aktualizowanymi przez Bank w komunikacie zamieszczonym w placówkach Banku oraz na stronie internetowej Banku.
3. Bank ma prawo zmiany numerów telefonów, pod którymi dokonywane są zastrzeżenia i blokowanie dostępu do bankowości internetowej, 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 bankowości internetowej.
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. Użytkownik może zachować ten sam identyfikator ID, pod warunkiem otrzymania od Banku nowego hasła dostępu.
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 osobiście w placówce Banku.

§ 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.
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

§ 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 bankowości internetowej 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 uwierzytłnił 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. Aplikacja mobilna Nasz Bank oraz Nasz Bank Junior

A. Korzystanie z aplikacji mobilnej

§ 20

1. Aplikacja mobilna Nasz Bank dostępna jest w sklepie Google Play dla systemu Android oraz App Store dla systemu IOS.

2. Po pobraniu i aktywacji aplikacji, użytkownik nadaje PIN do aplikacji oraz określa sposób logowania do aplikacji.
3. Logowanie do aplikacji może odbywać się za pomocą PIN-u do aplikacji lub identyfikacji danymi biometrycznymi.
4. Korzystanie z identyfikacji danymi biometrycznymi wymaga aktywacji tej funkcji na zaufanym urządzeniu mobilnym wraz z rejestracją indywidualnych cech fizycznych, a także aktywacji tej funkcji w aplikacji. Aplikacja nie przetwarza danych biometrycznych użytkownika.
5. Użytkownik może korzystać z aplikacji wyłącznie na zaufanym urządzeniu mobilnym.
6. Po pobraniu i aktywacji aplikacji mobilnej, użytkownik może autoryzować transakcje w aplikacji poprzez zatwierdzenie odpowiedniego komunikatu push (autoryzacja mobilna) lub hasłami SMS. W przypadku posiadania kilku urządzeń, powiadomienia push dotyczące autoryzacji będą wysyłane na wszystkie urządzenia mobilne z aktywną autoryzacją mobilną.
7. Aktywacja autoryzacji mobilnej w aplikacji Nasz Bank na urządzeniu samodzielnie przez użytkownika wymaga podania otrzymanego kodu SMS.
8. W przypadku wyboru autoryzacji transakcji w aplikacji mobilnej Nasz Bank, przywrócenie autoryzacji na hasła SMS użytkownik może dokonać:
 - 1) w placówce Banku,
 - 2) samodzielnie w Internet Banking – podczas wykonywania transakcji w serwisie Internet Banking i pojawienia się komunikatu dotyczącego wysłania powiadomienia autoryzacyjnego na urządzenie mobilne, zostanie wyświetlona możliwość przełączenia na autoryzację SMS; wybór tej opcji skutkuje wysłaniem wiadomości e-mail zawierającej kod do wpisania na stronie, po wprowadzeniu którego zostaną wyświetlone dodatkowe pytania weryfikujące; poprawna weryfikacja odpowiedzi spowoduje zmianę autoryzacji mobilnej na hasła SMS,
 - 3) poprzez rezygnację z aplikacji mobilnej, tj. świadome usunięcie przez klienta urządzenia mobilnego w Internet Bankingu lub usunięcie profilu w aplikacji mobilnej.
9. W przypadku zablokowania użytkownika (tj. 3-krotnego wpisania niewłaściwego e-PIN) lub odinstalowania aplikacji mobilnej Nasz Bank system nie zmieni sposobu autoryzacji klienta. Usunięcie ostatniego/jedynego urządzenia z aktywną autoryzacją mobilną spowoduje zmianę sposobu autoryzacji na SMS.
10. Po pobraniu i aktywacji aplikacji mobilnej Nasz Bank użytkownik, ze względów bezpieczeństwa, może mieć ograniczone czasowo niektóre funkcjonalności, np. nie może zmienić limitów transakcji w Internet Banking w ciągu 24 h ani dokonywać wypłat BLIK w bankomacie w ciągu 1h od momentu aktywacji tej aplikacji.
11. Wykonywanie przelewów, generowanie kodu BLIK oraz korzystanie ze smartKARTY w aplikacji mobilnej Nasz Bank możliwe jest wyłącznie na urządzeniach z aktywną autoryzacją mobilną.
12. Dezaktywacja aplikacji na zaufanym urządzeniu mobilnym jest jednoznaczna z odwołaniem przez użytkownika zgody na korzystanie z bankowości mobilnej na tym urządzeniu mobilnym. Usunięcie aplikacji mobilnej z urządzenia mobilnego bez uprzedniej dezaktywacji aplikacji nie jest równoznaczne z odwołaniem zgody na korzystanie z bankowości mobilnej. Sposób dezaktywacji aplikacji mobilnej opisany jest w *Przewodnikach po aplikacji*.
13. W przypadku nieudanego logowania poprzez identyfikację danymi biometrycznymi wymagane jest logowanie do aplikacji za pomocą PIN-u do tej aplikacji.
14. Błędne uwierzytelnienie użytkownika podczas logowania do aplikacji polegające na 3-krotnym wprowadzeniu błędnego PIN-u do aplikacji, powoduje automatyczne zablokowanie dostępu do aplikacji.
15. Licznik prób błędnego logowania jest zerowany po poprawnym zalogowaniu się do aplikacji, pod warunkiem, że nie nastąpiło zablokowanie dostępu do aplikacji.
16. Odblokowanie dostępu do aplikacji następuje poprzez:
 - 1) przeprowadzenie dezaktywacji i ponownej aktywacji aplikacji na zaufanym urządzeniu,
 - 2) w dowolnej placówce Banku przez pracownika Banku.
17. Małoletni użytkownik aplikacji instaluje i aktywuje aplikację mobilną Nasz Bank Junior za zgodą przedstawiciela ustawowego. Aktywacja aplikacji odbywa się zarówno w aplikacji Nasz Bank Junior jak i aplikacji rodzica – Nasz Bank.
18. Przedstawiciel ustawowy małoletniego zobowiązany jest do bieżącej weryfikacji prawidłowości przeprowadzanych przez małoletniego zleceń płatniczych i składanych do Banku dyspozycji.
19. Przedstawiciel ustawowy zobowiązany jest do wytłumaczenia małoletniemu zasad korzystania z aplikacji, w tym w szczególności zasad bezpieczeństwa aplikacji mobilnej oraz zasad dotyczących indywidualnych danych uwierzytelniających.
20. Szczegółowe funkcjonalności oraz zasady korzystania z aplikacji Nasz Bank oraz Nasz Bank Junior określają *Przewodniki po tych aplikacjach*.

B. Zasady bezpieczeństwa

§ 21

1. Użytkownik jest zobowiązany do:
 - 1) ochrony identyfikatora, hasła do bankowości internetowej, kodu SMS, PIN-u do aplikacji oraz zaufanego urządzenia mobilnego przed nieuprawnionym przejęciem lub użyciem przez osoby trzecie,
 - 2) niezwłocznego zgłoszenia utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia urządzenia mobilnego, na którym znajduje się aplikacja mobilna,
 - 3) niezwłocznego zgłoszenia nieuprawnionego użycia aplikacji mobilnej, usługi BLIK czy smartKARTY,
 - 4) niezwłocznego zgłoszenia Bankowi nieuprawnionego dostępu do rachunku za pomocą transakcji w ramach BLIK,
 - 5) nieudostępniania aplikacji mobilnej ani kodu BLIK osobom nieuprawnionym,
 - 6) nieudostępniania indywidualnych danych uwierzytelniających, w szczególności kodu autoryzacyjnego oraz jego ochrony,
 - 7) posługiwania się kodem BLIK zgodnie z jego przeznaczeniem,
 - 8) przechowywania PIN-u do aplikacji oraz urządzenia mobilnego, na którym została zainstalowana aplikacja mobilna z zachowaniem należytej staranności.
2. Zgłoszenie utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia urządzenia mobilnego z zainstalowaną aplikacją następuje:
 - 1) w oddziale Banku lub
 - 2) telefonicznie w godzinach pracy Banku.
3. Na podstawie zgłoszenia, o którym mowa ust. 2, Bank zastrzega usługę BLIK/smartKARTĘ lub dostęp do aplikacji mobilnej, co uniemożliwia posługiwanie się daną usługą/aplikacją na zaufanym urządzeniu mobilnym.
4. Zastrzeżenie dokonane jest bezterminowo, powodując brak możliwości dalszego korzystania z usługi/aplikacji.
5. Po dokonaniu zastrzeżenia usługi BLIK/usługi smartKARTY użytkownik może ponownie włączyć usługę BLIK/smartKARTĘ w aplikacji mobilnej, o ile nie nastąpiło zablokowanie dostępu do aplikacji.
6. Użytkownik może sam, w każdej chwili, zablokować/odblokować usługę BLIK/usługę smartKARTĘ w ustawieniach aplikacji poprzez wyłączenie/włączenie tej funkcjonalności.
7. Za udostępnienie zaufanego urządzenia mobilnego, udostępnienie aplikacji lub ujawnienie PIN-u do aplikacji osobom trzecim odpowiedzialność ponosi użytkownik aplikacji.
8. Użytkownik jest zobowiązany używać aplikacji pochodzącej z wiarygodnego źródła (wyłącznie ze sklepów Google Play oraz App Store).
9. Zaleca się, by użytkownik zapewnił ochronę zaufanego urządzenia mobilnego przy pomocy:
 - 1) blokady ekranu,
 - 2) programu antywirusowego.
10. Nie zaleca się otwierania na zaufanym urządzeniu mobilnym wiadomości e-mail, załączników do e-mail i linków do stron www, pochodzących z nieznanymi źródeł i od nieznanymi osób.
11. 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.
12. Nie należy instalować na urządzeniu mobilnym nielegalnych, nieznanymi programów, otrzymywanych pocztą e-mail lub pobranych ze stron internetowych.
13. Bank nigdy nie wymaga ujawnienia haseł oraz zainstalowania dodatkowego oprogramowania lub certyfikatów.
14. Użytkownik nie powinien korzystać z aplikacji mobilnej na urządzeniu mobilnym z usuniętymi fabrycznymi ograniczeniami systemowymi.

C. Ograniczenia w korzystaniu z aplikacji mobilnej

§ 22

- Bank uprawniony jest do czasowego zablokowania usługi BLIK/usługi smartKARTY/aplikacji mobilnej w przypadku:
 - uzasadnionych przyczyn związanych z bezpieczeństwem usługi,
 - stwierdzenia dokonania lub próby dokonania transakcji przez osobę nieuprawnioną,
 - użytkownika usługi w sposób niezgodny z prawem,
 - umyślnego doprowadzenia do nieautoryzowanych transakcji.
- Bank jest zobowiązany zablokować dostęp do aplikacji, uniemożliwiając tym samym wykonanie dyspozycji, w jednym z następujących przypadków:
 - złożenia przez użytkownika dyspozycji zablokowania lub dezaktywacji aplikacji;
 - 3-krotnego wprowadzenia nieprawidłowego PIN-u do aplikacji.
- Bank ma prawo częściowo ograniczyć lub zablokować dostęp do aplikacji i/lub czasowo zablokować wykonanie dyspozycji w następujących przypadkach:
 - uzasadnionych przyczyn związanych z bezpieczeństwem, tj.:
 - uzyskania informacji w tym podejrzenia, iż dyspozycje w aplikacji składane są przez osoby nieuprawnione,
 - zagrożenia przechwycenia danych dostępowych przez złośliwe oprogramowanie,
 - wykorzystywania danych dostępowych przez oprogramowanie automatycznie logujące się z dużą częstotliwością,
 - wykorzystywania systemów lub rachunków w sposób niezgodny z obowiązującymi przepisami prawa,
 - wykonywania działań mogących zagrażać bezpieczeństwu systemu i danych w nim przetwarzanych;
 - podejrzenia nieuprawnionego użycia aplikacji, zaufanego urządzenia mobilnego, indywidualnych danych uwierzytelniających lub umyślnego doprowadzenia do nieautoryzowanej dyspozycji;
 - powzięcia informacji o zagrożeniu bezpieczeństwa dyspozycji;
 - dokonywania czynności konserwacyjnych aplikacji lub innych systemów teleinformatycznych, związanych z korzystaniem z aplikacji, o czym Bank z wyprzedzeniem poinformuje użytkownika w aplikacji mobilnej;
 - dokonywania czynności mających na celu usunięcie awarii, usterek lub nieprawidłowości działania aplikacji lub innych systemów teleinformatycznych związanych z jej obsługą.
- Bank może uchylić ograniczenie albo blokadę dostępu do aplikacji w przypadku, o którym mowa w ust. 3 pkt 1-3, jeżeli na wniosek użytkownika, Bank wyda użytkownikowi nowe indywidualne dane uwierzytelniające.
- W przypadkach, o których mowa w ust. 3 pkt 2-5, ograniczenie lub blokada dostępu do aplikacji i/lub czasowa blokada dyspozycji następuje przez możliwie krótki okres niezbędny do usunięcia przyczyny ograniczenia lub blokady.
- Bank może zablokować dostęp do aplikacji w przypadku wygaśnięcia umów produktowych zawartych przez użytkownika z Bankiem.

§ 23

- Ze względów bezpieczeństwa wykonywania transakcji, Bank ma prawo wprowadzić kwotowe ograniczenia wysokości limitów transakcji wykonywanych w ramach usługi BLIK/usługi smartKARTA.
- Dzienne limity dla transakcji BLIK:

Rodzaj limitu BLIK	wartość standardowa	wartość maksymalna	limit ilościowy
Dzienny limit wypłat gotówki	500 PLN	5.000 PLN	10 szt
Dzienny limit transakcji bezgotówkowych	500 PLN	5.000 PLN	100 szt
w tym dzienny limit transakcji internetowych	500 PLN	5.000 PLN	100 szt
Limit pojedynczej transakcji przelew na telefon BLIK	500 PLN	500 PLN	
Dzienny limit wszystkich transakcji przelewów na telefon BLIK	5.000 PLN	5.000 PLN	
Dzienny limit globalny BLIK (przelewy, przelewy na telefon BLIK oraz próby o przelew BLIK)	5.000 PLN	5.000 PLN	

- Użytkownik może zawniekskować o indywidualne limity BLIK, z wyłączeniem limitu globalnego oraz limitów ilościowych.
- Limity dla transakcji w usłudze smartKARTA:

Rodzaj limitu	wartość standardowa
Dzienny limit wypłat gotówki	1.500 PLN
Limit pojedynczej wpłaty gotówki	5.000 PLN
Limit dzienny wpłat gotówki	20.000 PLN
Limit miesięczny wpłat gotówki	50.000 PLN

- Użytkownik może złożyć wniosek o indywidualne limity w usłudze smartKARTA. W przypadku złożenia przez klienta wniosku o zwiększenie limitu indywidualnego dla wpłat, decyzję podejmuje Dyrektor Oddziału.
- Podczas dokonywania wpłaty w bankomatach recyklingowych Bank może zapytać o źródło pochodzenia wpłacanych środków.

D. BLIK w aplikacji mobilnej

§ 24

- Usługa BLIK to usługa umożliwiająca dokonywanie transakcji BLIK za pomocą aplikacji mobilnej.
- Bank udostępnia usługę BLIK użytkownikowi bez konieczności składania dodatkowego wniosku. Aktywacja usługi BLIK odbywa się w aplikacji poprzez jej włączenie w ustawieniach.
- Z usługi BLIK może korzystać wyłącznie użytkownik, który pobrał na zaufanym urządzeniu aplikację mobilną.
- W celu korzystania z usługi BLIK użytkownik powinien łącznie spełnić następujące wymagania:
 - posiadać zaufane urządzenie mobilne,
 - posiadać rachunek w walucie PLN, w ciężar którego będą realizowane transakcje BLIK,
 - posiadać na urządzeniu mobilnym zainstalowaną aplikację mobilną,
 - włączyć w ustawieniach aplikacji usługę BLIK,
 - zaakceptować zasady funkcjonowania usługi.
- Użytkownik jest zobowiązany do korzystania z usługi BLIK w sposób zgodny z obowiązującym prawem, niniejszym regulaminem i *Przewodnikiem dla klienta po aplikacji mobilnej*.
- Użyte definicje mają następujące znaczenie:
 - baza powiązań BLIK – baza danych odbiorców przelewów na telefon BLIK prowadzona przez PSP;
 - kod BLIK – 6-cyfrowy kod niezbędny do realizowania transakcji w ramach usługi BLIK, generowany w aplikacji;
 - płatność BLIK – płatności za towary lub usługi w sklepie stacjonarnym/punkcie usługowym lub w sklepie internetowym z wykorzystaniem kodu BLIK, płatność BLIK jest poleceniem przelewu albo poleceniem przelewu wewnętrznego;
 - przelew na telefon BLIK – przelew krajowy, wykonywany na podstawie dyspozycji składanej w aplikacji, polegający na przekazaniu środków pieniężnych na konto odbiorcy zarejestrowanego w bazie powiązań BLIK i realizowany w czasie rzeczywistym w dniu złożenia dyspozycji przelewu, przelew na telefon BLIK jest poleceniem przelewu, użytkownik wykonując przelew podaje numer telefonu komórkowego odbiorcy;
 - prośba o przelew BLIK⁶ – przelew krajowy inicjowany przez nadawcę próby poprzez wysłanie komunikatu zawierającego prośbę o przelew kierowaną do użytkownika (nadawcy przelewu) za pośrednictwem PSP, który może zostać złożony wyłącznie przez użytkownika posiadającego aktywną usługę

⁶ Po udostępnieniu funkcjonalności przez Bank.

BLIK. Przelew ten jest wykonywany jedynie z rachunku powiązanego z usługą BLIK. Przelew na prośbę BLIK jest wykonywany na numer rachunku, do którego nadawca prośby jest uprawniony, na podstawie wskazanego w treści prośby numer telefonu. W tym rodzaju przelewu krajowego, unikatowym identyfikatorem jest numer telefonu, który jednoznacznie identyfikuje nadawcę prośby biorącego udział w tej transakcji płatniczej;

- 6) PSP – Polski Standard Płatności sp. z o.o. z siedzibą w Warszawie, będąca podmiotem zarządzającym i udostępniającym system BLIK;
- 7) transakcje BLIK – płatności BLIK, wypłaty BLIK i przelewy na telefon BLIK;
- 8) wypłata BLIK – transakcja BLIK polegająca na wypłacie środków pieniężnych w bankomacie lub w terminalu POS w sklepie stacjonarnym/punkcie usługowym, dokonywana bez użycia karty płatniczej, wypłata BLIK jest wypłatą gotówki.

§ 25

1. W ramach usługi BLIK mogą być realizowane następujące rodzaje transakcji:
 - 1) wypłata gotówki w bankomatach oznaczonych znakiem BLIK,
 - 2) wypłata gotówki w ramach usługi cash back w punktach handlowo-usługowych akceptujących BLIK,
 - 3) płatność za towary i usługi w polskich złotych:
 - a) w terminalach POS u akceptantów oznaczonych znakiem BLIK,
 - b) przez internet u akceptantów oznaczonych znakiem BLIK,
 - 4) wysyłanie przelewów na telefon BLIK,
 - 5) odbieranie przelewów na telefon BLIK,
 - 6) prośba o przelew BLIK⁷.
2. Użytkownik może realizować transakcje w ramach usługi BLIK do wysokości salda dostępnego na rachunku i w ramach limitów określonych dla transakcji BLIK.
3. Bank udostępni informacje o aktualnie obowiązujących limitach BLIK w niniejszym rozdziale.

E. Realizacja transakcji dokonywanych w usłudze BLIK

§ 26

1. Transakcje w usłudze BLIK:
 - 1) mogą być dokonywane w polskich złotych,
 - 2) są rozliczane na rachunkach prowadzonych w polskich złotych.
2. Dokonując transakcji w usłudze BLIK, użytkownik zobowiązany jest do jej autoryzacji na zasadach opisanych w ust. 4.
3. Za moment otrzymania przez Bank zlecenia płatniczego dotyczącego transakcji BLIK uznaje się moment dokonania autoryzacji transakcji BLIK przez użytkownika.
4. Użytkownik dokonuje autoryzacji transakcji BLIK – u akceptantów wyposażonych w terminal POS lub umożliwiających dokonanie transakcji BLIK w internecie, wykonując następujące czynności:
 - 1) uruchamia aplikację mobilną z użyciem kodu PIN dla aplikacji lub logowania biometrycznego,
 - 2) generuje kod BLIK w aplikacji mobilnej,
 - 3) wprowadza kod BLIK na terminalu POS lub na stronie internetowej,
 - 4) potwierdza transakcję BLIK w aplikacji mobilnej.
5. Przelew na telefon BLIK zostanie wykonany na numer rachunku, który jest przypisany w bazie powiązań BLIK do numeru telefonu komórkowego podanego przez użytkownika w aplikacji lub systemie bankowym. W celu otrzymywania przelewów na telefon BLIK użytkownik musi dodatkowo dokonać rejestracji w bazie powiązań BLIK, która polega na zapisaniu w niej numeru telefonu komórkowego oraz numeru rachunku, który będzie uznawany kwotą przelewu na telefon BLIK. Od chwili dokonania rejestracji w bazie powiązań BLIK, wszystkie przelewy na telefon BLIK wykonywane na numer telefonu podany w tej bazie są kierowane na rachunek płatniczy podany w bazie powiązań BLIK. Po zmianie numeru telefonu komórkowego użytkownik zarejestrowany w bazie powiązań BLIK w celu dalszego otrzymywania przelewów na telefon BLIK powinien zmienić swoje dane w bazie powiązań BLIK za pośrednictwem aplikacji. Tylko jeden numer telefonu może być powiązany przez użytkownika w bazie powiązań BLIK z numerem rachunku.
6. Prawidłowa dyspozycja przelewu na telefon BLIK, powinna zawierać:
 - 1) numer telefonu komórkowego odbiorcy przelewu;
 - 2) kwotę przelewu wyrażoną w PLN, nie wyższą niż kwota limitu dla tego typu zleceń płatniczych i nie wyższą niż kwota środków na danym rachunku płatnika;
 - 3) dane identyfikujące odbiorcę;
 - 4) tytuł przelewu na telefon BLIK.
7. Dyspozycja przelewu na prośbę BLIK⁸ może być złożona przez użytkownika po otrzymaniu w aplikacji mobilnej prośby o przelew od innego użytkownika lub klienta innego banku, który jest uprawniony do rachunku powiązanego z systemem rozliczeń BLIK. Użytkownik zlecający przelew występuje w charakterze płatnika, a przesyłający komunikat zawierający prośbę o przelew – zwany będzie nadawcą.
8. Prawidłowa prośba o przelew BLIK powinna zawierać:
 - 1) kwotę przelewu wyrażoną w PLN;
 - 2) tytuł przelewu;
 - 3) znane nadawcy i zapisane w urządzeniu mobilnym oznaczenie lub imię i nazwisko płatnika i jego numer telefonu powiązany z systemem rozliczeń BLIK. Na podstawie tej prośby Bank wyświetli płatnikowi dodatkowo imię i nazwisko nadawcy powiązane z jego numerem telefonu w banku nadawcy oraz dodatkowo bank może wyświetlić należący do nadawcy numer rachunku BLIK albo inny rachunek powiązany z systemem BLIK, do którego nadawca jest uprawniony.
9. Nadawca może anulować prośbę o przelew BLIK w aplikacji mobilnej najpóźniej przed autoryzacją przelewu przez płatnika. Prośba o przelew BLIK jest ważna 72 godziny od chwili wysłania jej przez nadawcę.
10. Bank umożliwia wysłanie więcej niż jednej prośby o przelew BLIK. Ze względów bezpieczeństwa Bank może jednak ograniczyć liczbę jednorazowo wysyłanych prośb o przelew.
11. Użytkownik może całkowicie wyłączyć możliwość odbierania prośb o przelew BLIK albo zablokować możliwość otrzymywania prośb o przelew BLIK od innego wskazanego użytkownika i określonego numeru telefonu. Blokada może być wycofana przez użytkownika.
12. Po otrzymaniu prośby o przelew BLIK płatnik może ją odrzucić albo zlecić przelew. Złożenie dyspozycji przelewu na prośbę BLIK następuje na wskazany w jej treści numer telefonu powiązany z nadawcą, na kwotę oraz tytuł wskazane przez nadawcę w treści komunikatu zawierającego prośbę o przelew.
13. Korzystanie z usługi BLIK wymaga:
 - 1) dla transakcji BLIK – wybrania rachunku, który będzie obciążany i uznawany kwotą transakcji BLIK,
 - 2) dla odbierania/wysyłania przelewów na telefon BLIK – rejestracji numeru telefonu komórkowego w bazie powiązań BLIK, który inni klienci mogą podawać jako unikatowy identyfikator w dyspozycjach przelewów na telefon BLIK w Banku,
 - 3) dla realizacji prośb o przelew BLIK – posiadania aktywnej usługi BLIK oraz rejestracji numeru telefonu komórkowego w bazie powiązań BLIK.
14. Użytkownik ma możliwość zmiany parametrów, o których mowa w ust. 13, w aplikacji mobilnej. Zmiana potwierdzana jest PIN-em do aplikacji.
15. Bank realizuje transakcje BLIK:
 - 1) przez całą dobę,
 - 2) w dniu jej otrzymania.
16. Bank odmawia przyjęcia realizacji transakcji BLIK w przypadku, gdy:
 - 1) rachunek wskazany do usługi BLIK został zamknięty,
 - 2) użytkownik podał nieprawidłowe dane podczas autoryzacji transakcji BLIK,

⁷ Po udostępnieniu funkcjonalności przez Bank.

⁸ Po udostępnieniu funkcjonalności przez Bank.

- 3) użytkownik przekroczył czas, wskazany w aplikacji mobilnej, w którym powinien dokonać zatwierdzenia transakcji,
- 4) przekroczony został czas ważności kodu BLIK,
- 5) kwota transakcji jest wyższa od limitu BLIK,
- 6) kwota transakcji jest wyższa od środków dostępnych na rachunku.
17. Akceptant ma prawo odmówić przyjęcia transakcji BLIK w przypadku, gdy:
 - 1) użytkownik podał nieprawidłowe dane podczas autoryzacji transakcji,
 - 2) nie można uzyskać zgody Banku na realizację transakcji BLIK.
18. Anulowanie transakcji BLIK możliwe jest do momentu dokonania przez użytkownika autoryzacji transakcji BLIK; po dokonaniu autoryzacji transakcji BLIK użytkownik może anulować transakcję BLIK wyłącznie u akceptanta, o ile akceptant oferuje taką możliwość.

§ 27

1. Wykorzystywany podczas autoryzacji kod BLIK:
 - 1) jest kodem jednorazowym ważnym maksymalnie 120 sekund od momentu jego wygenerowania, a informacja o zbliżającym się upływie czasu jego ważności jest podawana w aplikacji mobilnej,
 - 2) wygasa z upływem czasu jego ważności lub z chwilą autoryzacji transakcji BLIK, do której został wygenerowany.
2. Przelewy na telefon BLIK wychodzące z Banku są realizowane jako:
 - 1) przelewy wewnętrzne – w sytuacji, gdy rachunek odbiorcy jest rachunkiem prowadzonym w Banku,
 - 2) przelewy Express Elixir – w sytuacji, gdy rachunek odbiorcy nie jest rachunkiem prowadzonym w Banku.
3. Dyspozycje składane w aplikacji przez użytkownika wymagają autoryzacji z użyciem indywidualnych danych uwierzytelniających:
 - 1) PIN-u do aplikacji lub
 - 2) identyfikacji danymi biometrycznymi,
 - 3) w przypadku dyspozycji składanych przez małoletniego także zgody przedstawiciela ustawowego małoletniego.
4. Autoryzacja zlecenia płatniczego BLIK przez użytkownika oznacza jego zgodę na wykonanie transakcji płatniczej. Cofnięcie zgody od chwili autoryzacji nie jest możliwe.

F. BLIK w aplikacji Nasz Bank Junior

§ 28

1. Rodzic może udostępnić dziecku kod BLIK po włączeniu ustawień dot. udostępniania kodu BLIK w swojej aplikacji mobilnej Nasz Bank. Transakcja BLIK przebiega w następujący sposób:
 - 1) dziecko w aplikacji mobilnej Nasz Bank Junior wysyła prośbę o kod BLIK,
 - 2) rodzic potwierdza prośbę o kod BLIK w swojej aplikacji,
 - 3) kod BLIK zostaje wyświetlony w aplikacji Nasz Bank Junior, który dziecko podaje podczas płatności,
 - 4) rodzic potwierdza płatność wykonaną przez dziecko przy użyciu kodu BLIK.
2. Dienne limity dla transakcji BLIK:

Rodzaj limitu BLIK	wartość standardowa	wartość maksymalna	limit ilościowy
Dzienny limit wypłat gotówki	500 PLN	500 PLN	10 szt
Dzienny limit transakcji bezgotówkowych w tym dzienny limit transakcji internetowych	500 PLN	500 PLN	100 szt
Dzienny limit globalny BLIK	5.000 PLN	5.000 PLN	100 szt

G. Usługa smartKARTA w aplikacji mobilnej

§ 29

1. Usługa smartKARTA to usługa umożliwiająca dokonywanie transakcji w bankomacie/bankomacie recyklingowym Banku przy pomocy wygenerowanego w aplikacji mobilnej Nasz Bank kodu QR, bez dotykania urządzenia.
2. Bank udostępnia usługę smartKARTA użytkownikowi bez konieczności składania dodatkowego wniosku. Aktywacja usługi odbywa się w aplikacji poprzez włączenie jej w ustawieniach.
3. Z usługi smartKARTA może korzystać wyłącznie użytkownik, który pobrał na zaufanym urządzeniu aplikację mobilną Nasz Bank.
4. W celu korzystania z usługi smartKARTA użytkownik powinien łącznie spełnić następujące wymagania:
 - 1) posiadać zaufane urządzenie mobilne,
 - 2) posiadać rachunek w walucie PLN, w ciężar którego będą realizowane transakcje,
 - 3) posiadać na urządzeniu mobilnym zainstalowaną aplikację mobilną Nasz Bank.
5. Użytkownik jest zobowiązany do korzystania z usługi smartKARTA w sposób zgodny z obowiązującym prawem, niniejszym regulaminem i *Przewodnikiem po aplikacji mobilnej*.

§ 30

1. W ramach usługi smartKARTA mogą być realizowane następujące rodzaje transakcji:
 - 1) wypłata gotówki w bankomatach własnych Banku,
 - 2) wpłata gotówki w bankomatach recyklingowych Banku. Wykaz bankomatów recyklingowych obsługujących wpłatę gotówki znajduje się na stronie internetowej Banku: www.bszl.com.pl.
2. Użytkownik może realizować transakcje w ramach usługi smartKARTA do wysokości salda dostępnego na rachunku i w ramach limitów określonych dla transakcji w usłudze smartKARTA.

H. Realizacja transakcji dokonywanych w usłudze smartKARTA

§ 31

1. Transakcje w usłudze smartKARTA:
 - 1) mogą być dokonywane w polskich złotych,
 - 2) są rozliczane na rachunkach prowadzonych w polskich złotych.
2. Dokonując transakcji w usłudze smartKARTA, użytkownik zobowiązany jest do jej autoryzacji na zasadach opisanych w ust. 4.
3. Za moment otrzymania przez Bank zlecenia płatniczego dotyczącego transakcji w usłudze smartKARTA uznaje się moment dokonania autoryzacji transakcji w usłudze smartKARTA przez użytkownika.
4. Użytkownik dokonuje autoryzacji transakcji w usłudze smartKARTA w bankomatach/bankomatach recyklingowych Banku, w następujący sposób:
 - 1) uruchamia aplikację mobilną Nasz Bank z użyciem kodu PIN dla aplikacji lub logowania biometrycznego,
 - 2) wybiera w aplikacji właściwą funkcję (wpłata/wypłata) wraz z kwotą transakcji,
 - 3) skanuje kod QR wyświetlony w bankomacie/bankomacie recyklingowym,
 - 4) potwierdza transakcję w aplikacji mobilnej Nasz Bank.
5. Bank realizuje transakcje w usłudze smartKARTA:
 - 1) przez całą dobę,
 - 2) w dniu jej otrzymania.
6. Bank odmawia przyjęcia realizacji transakcji w usłudze smartKARTA w przypadku, gdy:
 - 1) użytkownik podał nieprawidłowe dane podczas autoryzacji transakcji,
 - 2) użytkownik przekroczył czas, wskazany w aplikacji mobilnej, w którym powinien dokonać zatwierdzenia transakcji,
 - 3) kwota transakcji jest wyższa od limitu w usłudze smartKARTA,

- 4) kwota transakcji jest wyższa od środków dostępnych na rachunku.
7. Anulowanie transakcji smartKARTA możliwe jest do momentu dokonania przez użytkownika autoryzacji transakcji. Po dokonaniu autoryzacji użytkownik nie może anulować transakcji.

I. Funkcjonalności dostępne w aplikacji mobilnej Nasz Bank i Nasz Bank Junior

§ 32

1. Szczegółowe funkcjonalności dostępne w aplikacji mobilnej Nasz Bank Junior przedstawia tabela:

	Funkcjonalność	Dostępność	Informacje dodatkowe
1.	Podgląd rachunków	tak	
2.	Zakładanie skarbonek	tak	
3.	Dozwolone operacje: 1) przelew memorialowy 2) przelew wyjściowy 3) przelew wejściowy 4) transakcje BLIK	tak	
4.	Podgląd karty płatniczej	tak	
5.	Usługa BLIK (płatności w sklepach stacjonarnych, internetowych, wypłaty gotówki w bankomatach)	tak	rodzic udostępnia kod BLIK i akceptuje transakcje w aplikacji Nasz Bank
6.	Zmiana limitów BLIK	tak	zmiana możliwa przez rodzica w aplikacji Nasz Bank
7.	Zmiana limitów karty płatniczej	tak	zmiana możliwa przez rodzica w aplikacji Nasz Bank
8.	Obsługa karty płatniczej (blokowanie, zastrzeganie)	tak	funkcje dostępne dla rodzica w aplikacji Nasz Bank
9.	Doładowanie telefonu na kartę	tak	funkcja dostępna dla rodzica w aplikacji Nasz Bank
10.	Mapa nagród	tak	automatyczne nagradzanie za aktywności i aktywne oszczędzanie
11.	Pełna kontrola rodzica	tak	rodzic na swojej aplikacji ma dostęp do produktów dziecka
12.	Inne funkcjonalności, niewykazane w niniejszej tabeli, zostały opisane w przewodniku po aplikacji mobilnej Nasz Bank Junior.		

2. Szczegółowe funkcjonalności dostępne w aplikacji mobilnej Nasz Bank przedstawia tabela:

Funkcjonalność		Dostępność		Informacje dodatkowe
		IB	IBF	
1.	Podgląd			
	1) lista rachunków (ROR, rachunek oszczędnościowy, lokata, kredyt)	tak	tak	
	2) historia, saldo i dostępne środki	tak	tak	
	3) szczegóły rachunku	tak	tak	
	4) karty płatnicze	tak	tak	wyłącznie debetowe karty wydane do rachunku
	5) blokady transakcji kartą płatniczą	tak	tak	
2.	Przelewy			
	1) przelew własny	tak	tak	
	2) przelew krajowy	tak	tak	
	3) przelew US/ZUS	tak	tak	
	4) przelew dewizowy europejski	tak	tak	wyłącznie przelew w walucie EUR
	5) doładowanie telefonu	tak	tak	
	6) przelew QR	tak	tak	
3.	Lokaty			
	1) podgląd	tak	tak	
	2) założenie lokaty	tak	nie	
	3) likwidacja lokaty	tak	nie	wyłącznie lokaty założone w IB
4.	Kredyty			
	1) podgląd	tak	tak	
	2) wniosek o kredyt	nie	nie	
	3) spłata kredytu	nie	nie	
5.	Usługi kartowe			
	1) nadanie/zmiana PINu do karty płatniczej	tak	tak	
	2) zmiana statusu karty płatniczej			
	a) aktywacja	tak	tak	
	b) zablokowanie	tak	tak	
	c) odblokowanie	tak	tak	
	d) zastrzeżenie	tak	tak	
	3) zmiana limitów	tak	tak	pod warunkiem, że użytkownik karty ma do tego prawo
	4) włączenie/wyłączenie płatności zbliżeniowych	tak	nie	
	5) zamówienie karty płatniczej	tak	nie	
6.	Pozostałe usługi			
	1) smartKARTA	tak	tak	wykaz bankomatów obsługujących wpłaty i wypłaty za pomocą smartKARTY na stronie: www.bszl.com.pl

2) transakcja przy użyciu kodu BLIK	tak	tak	BLIK w IBF w wariantcie wieloosobowej autoryzacji transakcji – po udostępnieniu przez Bank na wniosek klienta
3) przelew BLIK na numer telefonu	tak	tak	
4) mobilna autoryzacja operacji dokonywanych w IB	tak	tak	
5) mobilna autoryzacja operacji dokonywanych w placówce Banku	tak	tak	możliwe do zatwierdzenia wpłaty i wypłaty kasowe oraz przelewy
6) potwierdzenie transakcji internetowej dokonanej kartą płatniczą z wykorzystaniem usługi 3D Secure	tak	nie	wyłącznie debetowe karty wydane do rachunku
7) wysłanie wiadomości do Banku	tak	tak	
8) mobilne potwierdzanie tożsamości pracownika Banku	tak	tak	
9) Kantor SGB	tak	tak	
10) zarządzanie aplikacją dziecka – Nasz Bank Junior	tak	nie	
7. Ustawienia			
1) włączenie/wyłączenie BLIKa	tak	tak	
2) zmiana limitów BLIK	nie	nie	
3) rejestracja numeru telefonu w usłudze przelew BLIK na telefon	tak	tak	
4) zmiana limitu wypłaty dla smartKARTY	nie	nie	
5) zmiana PINu do aplikacji	tak	tak	
6) wybór informacji widocznych przed zalogowaniem	tak	tak	
7) wybór metody logowania do aplikacji	tak	tak	
8) zablokowanie kanału dostępu	tak	tak	
8. Inne funkcjonalności, niewykazane w niniejszej tabeli, zostały opisane w przewodniku po aplikacji mobilnej Nasz Bank.			

3. Pracownik Banku może wysłać użytkownikowi aplikacji mobilnej Nasz Bank komunikat push w formie powiadomienia (informacji) lub żądania autoryzacji.
4. Komunikat, o którym mowa w ust. 3, może służyć m.in. do:
- 1) poinformowania użytkownika o planowanym kontakcie pracownika Banku z klientem – pracownik Banku, uprzedzając kontakt telefoniczny z klientem, wysłać użytkownikowi aplikacji mobilnej Nasz Bank komunikat push informujący o planowanym kontakcie Banku podając szczegółowe informacje (imię i nazwisko pracownika, dane placówki Banku, datę planowanego kontaktu, cel rozmowy);
 - 2) wyrażenia/niewyrażenia zgody na kontakt pracownika Banku z klientem – pracownik Banku wysłać informacje, o których mowa w pkt 1, oraz dodatkowo prosi o potwierdzenie bądź odrzucenie komunikatu;
 - 3) potwierdzenia tożsamości pracownika Banku w przypadku kontaktu pracownika z klientem – podczas rozmowy telefonicznej z klientem pracownik Banku wysłać komunikat push ze swoimi danymi;
 - 4) potwierdzenia tożsamości użytkownika aplikacji w przypadku kontaktu klienta z Bankiem – w celu weryfikacji danych klienta pracownik Banku wysłać komunikat z prośbą o potwierdzenie danych użytkownika w aplikacji.

Rozdział 8. Standardowe maksymalne limity pojedynczej transakcji oraz limity wszystkich transakcji w ciągu dnia

§ 33

1. Standardowe maksymalne limity pojedynczej transakcji oraz limity wszystkich transakcji w ciągu dnia dokonywanych za pośrednictwem bankowości internetowej:

Limity w Internet Banking – IB			
Kanał dostępu		Limit pojedynczej transakcji	Limit wszystkich transakcji w ciągu dnia
Limity do rachunku w walucie PLN			
Aplikacja mobilna		1 000,00 zł (istnieje możliwość zwiększenia limitu za pośrednictwem IB do 3 000,00 zł na 10 min.)	3 000,00 zł
Serwis internetowy	Płatności ekspresowe BlueCash	3 000,00 zł	5 szt. (łącznie w IB i w Banku)
	Płatności ekspresowe Express Elixir	3 000,00 zł	5 szt. (łącznie w IB i w Banku)
	Przelew standardowy	5 000,00 zł (w przypadku posiadania niższego limitu istnieje możliwość zwiększenia limitu za pośrednictwem IB do 5 000,00 zł na 10 min.)	20 000,00 zł
	Łączny limit IB:	5 000,00 zł	20 000,00 zł
Limity do rachunku w walucie wymiennej EUR/USD/GBP			
Serwis internetowy (IB)		2 000,00 EUR/USD/GBP	5 000,00 EUR/USD/GBP
Aplikacja mobilna		1 000,00 EUR/USD/GBP	2 000,00 EUR/USD/GBP
Limity w Internet Banking dla Firm – IBF (rady rodziców, SKO, KZP)			
Kanał dostępu		Limit pojedynczej transakcji	Limit wszystkich transakcji w ciągu dnia
Limity do rachunku w walucie PLN			

Aplikacja mobilna		autoryzacja przelewów: do wysokości limitu w IB wprowadzanie przelewów: 1 000,00 zł	autoryzacja przelewów: do wysokości limitu w IB wprowadzanie przelewów: 3 000,00 zł
Serwis internetowy	Płatności ekspresowe BlueCash	3 000,00 zł	5 szt. (łącznie w IB i w Banku)
	Płatności ekspresowe Express Elixir	3 000,00 zł	5 szt. (łącznie w IB i w Banku)
	Przelew standardowy	5 000,00 zł (w przypadku posiadania niższego limitu istnieje możliwość zwiększenia limitu za pośrednictwem IBF do 5 000,00 zł na 10 min.)	20 000,00 zł
	Łączny limit IBF:	5 000,00 zł	20 000,00 zł
Limity do rachunku w walucie wymiennej EUR/USD/GBP			
Serwis internetowy (IB)		2 000,00 EUR/USD/GBP	5 000,00 EUR/USD/GBP
Aplikacja mobilna		1 000,00 EUR/USD/GBP	2 000,00 EUR/USD/GBP

2. Limity dotyczą transakcji na rachunku.
3. Z zastrzeżeniem ust. 4, użytkownik może wnioskować o indywidualne ustalenie limitów, o których mowa w ust. 1.
4. O wysokości limitów ostatecznie decyduje Bank.
5. Przelewy wewnętrzne pomiędzy rachunkami klienta nie są wliczane do limitów, o których mowa w ust. 1.

Rozdział 9. Inne postanowienia

§ 34

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 podlegania do popełniania czynów zabronionych, w szczególności do wprowadzania do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł.

Załącznik nr 3

do „Regulaminu świadczenia usług w zakresie prowadzenia rachunków bankowych dla klientów instytucjonalnych w Banku Spółdzielczym Ziemi Łowickiej w Łowiczu”

Zasady udostępniania i funkcjonowania elektronicznych kanałów dostępu

Spis treści

Rozdział 1. Udostępnienie i warunki korzystania z elektronicznych kanałów dostępu	12
Rozdział 2. Dyspozycje składane za pośrednictwem elektronicznych kanałów dostępu	13
A. Dyspozycje ogólne	13
B. Autowypłata	15
Rozdział 3. Korzystanie z usług bankowości elektronicznej	15
Rozdział 4. Ograniczenia w korzystaniu z usług bankowości elektronicznej	15
Rozdział 5. Blokowanie i zastrzeżenie dostępu do bankowości internetowej	16
Rozdział 6. Udostępnianie informacji na potrzeby świadczenia usług inicjowania transakcji płatniczych i usług dostępu do informacji o rachunku	16
Potwierdzanie dostępności środków na rachunku	16
Rozdział 7. Aplikacja mobilna Nasz Bank	17
A. Korzystanie z aplikacji mobilnej	17
B. Zasady bezpieczeństwa	17
C. Ograniczenia w korzystaniu z aplikacji mobilnej	18
D. BLIK w aplikacji mobilnej	18
E. Realizacja transakcji dokonywanych w usłudze BLIK	19
F. Usługa smartKARTA w aplikacji mobilnej Nasz Bank	20
G. Realizacja transakcji dokonywanych w usłudze smartKARTA	20
H. Funkcjonalności dostępne w aplikacji mobilnej Nasz Bank	21
Rozdział 8. Standardowe limity pojedynczej transakcji oraz limity wszystkich transakcji w ciągu dnia	22
Rozdział 9. Inne postanowienia	22

Rozdział 1. Udostępnienie i warunki korzystania z elektronicznych kanałów dostępu

§ 1

1. Bank może świadczyć usługi w zakresie obsługi produktów i usług za pośrednictwem następujących elektronicznych kanałów dostępu:
 - a) serwis internetowy – dostęp do bankowości internetowej poprzez sieć internet (kanał www),
 - b) interfejs mobilny⁹ – dostęp do bankowości internetowej poprzez sieć internet (kanał www) na urządzeniu mobilnym (smartfon, tablet),
 - c) aplikacja mobilna¹⁰ – dostęp do bankowości internetowej przy pomocy aplikacji pobranej na urządzeniu mobilnym;
- 2) usługa SMS Banking – uzyskiwanie informacji związanych z transakcjami na rachunku w formie wiadomości SMS; wiadomości w usłudze SMS Banking wysyłane są codziennie w godz. 6:00-22:00.
2. Informacje o produktach i usługach dostępnych za pośrednictwem bankowości internetowej znajdują się na stronie internetowej Banku.

⁹ Nie dotyczy IBF.

¹⁰ W przypadku IBF funkcjonalności dostępne w aplikacji mobilnej Nasz Bank zostały wskazane w § 32.

3. Warunki korzystania z usług bankowych w bankowości internetowej określa *Przewodnik dla klienta*, natomiast warunki korzystania z usług w bankowości mobilnej określają instrukcje: *Interfejs mobilny Internet Bankingu* oraz instrukcja użytkownika *Aplikacja mobilna Nasz Bank*.
4. Instrukcje, o których mowa ust. 3, zawierają opisy poszczególnych elektronicznych kanałów dostępu, wymagania techniczne dla każdego kanału i zasady prawidłowego posługiwania się tymi kanałami przez klienta. Przewodniki są udostępnione na stronie internetowej Banku oraz wydawane na życzenie klienta przy zawieraniu umowy.
5. Zakres funkcjonalny serwisu internetowego, o którym mowa w ust. 1 pkt 1, jest dostępny w dwóch wariantach:
 - 1) wariant I – z jednoosobową autoryzacją dyspozycji (IB – Internet Banking);
 - 2) wariant II – z jedno lub wieloosobową autoryzacją dyspozycji (IBF – Internet Banking dla Firm).
6. Użytkownik systemu może korzystać z dostępu do bankowości internetowej za pomocą kanału www, interfejsu mobilnego lub aplikacji mobilnej na podstawie tego samego ID wydanego w Banku.

§ 2

1. Usługi bankowości elektronicznej mogą być udostępniane w przypadku posiadania przez posiadacza rachunku bieżącego prowadzonego w złotych. W przypadku rachunku rozliczeniowego w walucie wymienialnej warunkiem udostępnienia elektronicznych kanałów dostępu jest posiadanie rachunku rozliczeniowego w walucie PLN, z którego będą pobierane prowizje i opłaty.
2. Lokaty i kredyty również mogą zostać udostępnione w elektronicznych kanałach dostępu na życzenie klienta, o ile wcześniej uruchomiono bankowość internetową. Szczegółowy zakres funkcjonalności lokat i kredytów w elektronicznych kanałach dostępu został opisany w *Przewodnikach dla klientów*.
3. 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 aktualnej ofercie znajdują się na stronie internetowej Banku, natomiast informacje o dostępnych sposobach zawierania umów określa regulamin.
4. Bank udostępnia Kantor SGB dla użytkownika korzystającego z Internet Banking lub Internet Banking dla Firm; zasady świadczenia usługi Kantor SGB w ramach usługi bankowości elektronicznej stanowią załącznik nr 4 do regulaminu.
5. Bank może udostępnić użytkownikowi systemu węższy zakres usługi niż wynikałby on z jego wniosku, jeżeli decyzja Zarządu Banku o ograniczeniu zakresu usługi uzasadniona jest względami bezpieczeństwa Banku lub oceną dotychczasowej współpracy z posiadaczem rachunku.

§ 3

1. Użytkownik uzyskuje dostęp do bankowości elektronicznej za pomocą indywidualnych danych uwierzytelniających.
2. Bank może umożliwić korzystanie z usługi przy użyciu tych samych indywidualnych danych uwierzytelniających użytkownikowi, będącemu równocześnie posiadaczem/ppełnomocnikiem do innego rachunku, z uwzględnieniem limitów operacji, o których mowa w § 33.

§ 4

1. W przypadku korzystania i dokonywania transakcji z wykorzystaniem bankowości internetowej:
 - 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 *Przewodnikach dla klienta*.
3. Użytkownikiem, niebędącym posiadaczem rachunku może być osoba, której posiadacz rachunku udzielił odpowiedniego pełnomocnictwa; użytkownikiem może być również inna osoba wskazana przez posiadacza rachunku, niebędąca pełnomocnikiem, którą posiadacz rachunku wskazał jako pasywnego użytkownika.
4. Warunkiem korzystania z usługi jest obsługa plików *cookies* w przeglądarce internetowej, które są konieczne do utrzymania aktywnej sesji po zalogowaniu do bankowości internetowej; szczegółowe informacje dotyczące rodzaju stosowanych plików *cookies* oraz celu ich wykorzystywania dostępne są na stronie internetowej Banku.

§ 5

1. Użytkownik/pasywny użytkownik ma obowiązek korzystać z elektronicznych kanałów dostępu zgodnie z umową, regulaminem oraz *Przewodnikami dla klienta*, a także 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 zapobieganiu 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

1. Bank, w przypadku wyrażenia zgody przez Klienta, umożliwia skorzystanie z metody Device Fingerprinting (DFP)¹¹, która identyfikuje użytkownika po urządzeniu, z którego się loguje. Urządzenie zostaje oznaczone jako zaufane, dzięki czemu logując się z tego urządzenia Klient nie musi stosować metod silnego uwierzytelnienia.
2. Klient powinien być jedynym użytkownikiem urządzenia, które oznaczane jest jako zaufane.
3. Szczegółowe informacje odnośnie metody DFP zostały określone w *Przewodniku dla klienta*.

§ 7

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

Rozdział 2. Dyspozycje składane za pośrednictwem elektronicznych kanałów dostępu

A. Dyspozycje ogólne

§ 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, przy uwzględnieniu wymogów silnego uwierzytelniania.

§ 9

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 § 10 - § 14 niniejszego załącznika oraz sposobów posługiwania się danym elektronicznym kanałem dostępu opisanych w *Przewodnikach dla klienta*.
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.

¹¹ Nie dotyczy IBF.

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 w serwisie internetowym:
 - 1) wymianę walut w Kantorze SGB użytkownikom, którym Bank udostępnił usługę, zgodnie z zasadami określonymi w załączniku nr 4 do regulaminu;
 - 2) składanie wniosku o wypłatę świadczenia wychowawczego – dostępność usługi dla kanału IB, uzależniona od współpracy z Ministerstwem Rodziny i Polityki Społecznej;
 - 3) składanie wniosku o terminal POS¹²;
 - 4) składanie innych wniosków udostępnionych przez Bank.

§ 10

1. Wszelkie dyspozycje i zlecenia płatnicze w bankowości internetowej, 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 internetowej, użytkownik dokonuje ich autoryzacji przy użyciu indywidualnych danych uwierzytelniających, z zastosowaniem wymaganych przez Bank metod uwierzytelniania.
 3. Autoryzacja dokonana przez użytkownika systemu jest równoznaczna z poleceniem Bankowi dokonania określonej czynności i stanowi podstawę jej dokonania.
 4. Bank zastrzega sobie prawo skontaktowania się z użytkownikiem w celu realizacji zlecenia płatniczego.
 5. 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 6.
 6. 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. 7;
 - 2) inicjowania transakcji, której odbiorca znajduje się na liście zaufanych odbiorców utworzonej uprzednio przez użytkownika;
 - 3) inicjowania kolejnych transakcji należących do serii transakcji cyklicznych, opiewających na tę samą kwotę na rzecz tego samego odbiorcy, pod warunkiem, że utworzenie, zmiana lub zainicjowanie pierwszej transakcji cyklicznej odbyło się przy zastosowaniu silnego uwierzytelniania;
 - 4) jeżeli użytkownik inicjuje transakcję płatniczą w sytuacji, gdy płatnik i odbiorca są tą samą osobą fizyczną lub prawną i oba rachunki płatnicze są prowadzone przez Bank,
 - 5) inicjowania zdalnej transakcji, którą Bank uzna za charakteryzującą się niskim poziomem ryzyka zgodnie z mechanizmami monitorowania transakcji.
 7. Bank stosuje silne uwierzytelnianie użytkownika, jeżeli spełniony jest którykolwiek z następujących warunków:
 - 1) użytkownik/pasywny użytkownik uzyskuje dostęp do informacji określonych w ust. 6 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. 6 pkt 1 lit. b) w trybie online oraz odkąd ostatni raz zastosowano silne uwierzytelnianie użytkownika/pasywnego użytkownika.
 8. Dostęp użytkownika do serwisu internetowego następuje poprzez podanie identyfikatora oraz udostępnionych użytkownikowi/pasywnemu użytkownikowi indywidualnych danych uwierzytelniających, o których mowa w ust. 9.
 9. Dostęp oraz autoryzacja dyspozycji składanych za pośrednictwem bankowości internetowej przez użytkownika/ pasywnego użytkownika odbywa się poprzez użycie następujących indywidualnych danych uwierzytelniających:
 - 1) dla wariantu I, o którym mowa w § 1 ust. 5 pkt 1:
 - a) identyfikatora ID (loginu);
 - b) hasła stałego i hasła SMS;
 - c) mObywatel¹³;
 - d) klucza bezpieczeństwa U2F;
 - e) kodu uwierzytelniającego;
 - f) tokena Athena wraz z aplikacją nPodpis (wymogi dotyczące instalacji aplikacji nPodpis na komputerze klienta opisane są w instrukcji użytkownika *Aplikacja nPodpis do obsługi certyfikatu*);
 - g) hasła do tokena Vasco DIGIPASS GO3 i aktualnego wskazania tokena – dotyczy pasywnego użytkownika systemu;
 - h) aplikacji mobilnej Nasz Bank i zatwierdzenie transakcji w tej aplikacji; (wymogi dotyczące instalacji aplikacji na urządzeniu mobilnym opisane są w instrukcji użytkownika *Aplikacja mobilna Nasz Bank*) lub
 - 2) dla wariantu II, o którym mowa w § 1 ust. 5 pkt 2:
 - a) identyfikatora ID (loginu);
 - b) hasła stałego i hasła SMS;
 - c) mObywatel¹³;
 - d) klucza bezpieczeństwa U2F;
 - e) kodu uwierzytelniającego;
 - f) tokena Athena wraz z aplikacją nPodpis nPodpis (wymogi dotyczące instalacji aplikacji nPodpis na komputerze klienta opisane są w instrukcji użytkownika *Aplikacja nPodpis do obsługi certyfikatu*);
 - g) hasła do tokena DIGIPASS GO3 i aktualnego wskazania tokena – dotyczy pasywnego użytkownika systemu;
 - h) aplikacji mobilnej Nasz Bank i zatwierdzenie transakcji w tej aplikacji (wymogi dotyczące instalacji aplikacji na urządzeniu mobilnym opisane są w instrukcji użytkownika *Aplikacja mobilna Nasz Bank*);
- chyba że Bank udostępni inne indywidualne dane uwierzytelniające, które są opisane w *Przewodnikach dla klienta*.
10. Hasło stałe, o którym mowa w ust. 9, jest nadawane przez użytkownika, podczas procesu pierwszego logowania do bankowości internetowej, po przekazaniu przez Bank hasła tymczasowego. Bank określa w *Przewodnikach dla klienta* zasady tworzenia hasła stałego (składniki hasła stałego).
 11. Bank umożliwia logowanie do systemu bankowości internetowej za pomocą aplikacji mObywatel¹³ lub klucza bezpieczeństwa U2F. Sposób logowania tymi metodami oraz sposób dodawania klucza bezpieczeństwa został opisany w *Przewodnikach dla klienta*.
 12. Użytkownik może modyfikować listę aktywowanych kluczy bezpieczeństwa U2F poprzez dodawanie lub usuwanie poszczególnych kluczy z listy kluczy zabezpieczeń dostępnej w bankowości internetowej.
 13. 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

¹² Dla usługi IBF opcja dostępna po wdrożeniu funkcjonalności przez Bank.

¹³ Usługa dostępna po wdrożeniu przez Bank.

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

14. 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 lub autoryzacji mobilnej.
15. Użytkownik ma możliwość samodzielnego ustanowienia nowego hasła do serwisu internetowego, np. w przypadku zapomnienia dotychczasowego hasła. Zmiana hasła możliwa jest podczas logowania do bankowości internetowej. Wybór tej opcji skutkuje koniecznością wpisania identyfikatora ID, a następnie numeru telefonu. Po poprawnym wprowadzeniu danych zostanie wysłany e-mail zawierający kod do wpisania na stronie, po wprowadzeniu którego zostaną wyświetlone dodatkowe pytania weryfikujące. Poprawna weryfikacja odpowiedzi spowoduje wysłanie wiadomości SMS zawierającej nowe hasło. Logowanie z jego użyciem wymusi zmianę hasła. Numer telefonu oraz adres e-mail muszą być zgodne z danymi podanymi w Banku.
16. 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 *Przewodnikach dla klienta*.
17. W przypadku autoryzacji hasłami SMS Bank przysyła kody autoryzacyjne (hasła SMS) wykorzystywane przy stosowanych metodach uwierzytelniania na numer telefonu komórkowego, który użytkownik wskazał w Banku.

§ 11

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

§ 12

1. Realizacja dyspozycji składanych za pośrednictwem bankowości internetowej 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 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;
 - 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.

B. Autowypłata

§ 13a

1. Bank udostępnia w Internet Banking dla Firm usługę autowypłaty, która polega na przygotowaniu wypłaty do realizacji w kasie w placówce Banku dla dowolnej osoby fizycznej, podając:
 - 1) imię i nazwisko,
 - 2) PESEL,
 - 3) numer dokumentu tożsamości,
 - 4) adres.
2. Wypłata w usłudze autowypłaty odbywa się w kasie Banku na podstawie ważnego dokumentu tożsamości w ściśle określonej kwocie oraz w przedziale czasowym ustalonym przez użytkownika IBF.
3. Zlecenia w usłudze autowypłaty wymagają autoryzacji zgodnie z wydanymi indywidualnymi danymi uwierzytelniającymi i liczbą wymaganych podpisów.
4. Osoba fizyczna, o której mowa w ust. 1, dokonuje wypłaty w kasie Banku na podstawie ważnego dokumentu tożsamości, który został podany przez użytkownika IBF.
5. Szczegóły dotyczące usługi autowypłaty opisuje *Przewodnik dla klienta*.

§ 14

1. Bank ma prawo odmowy wykonania dyspozycji złożonej i uwierzytelnionej w bankowości internetowej 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

§ 15

Za pośrednictwem elektronicznych kanałów dostępu użytkownik/pasywny użytkownik uzyskuje dostęp do wszystkich rachunków otwartych przed dniem aktywowania usługi oraz do rachunków otwartych w terminie późniejszym, chyba że posiadacz rachunku, zawnioskował o ograniczony dostęp do rachunków, za pośrednictwem elektronicznych kanałów dostępu. Bank może automatycznie udostępnić posiadaczowi rachunku i/lub pełnomocnikowi nowo otwarte rachunki ROR, rachunki lokat oraz rachunki kredytów bez konieczności składania wniosku.

Rozdział 4. Ograniczenia w korzystaniu z usług bankowości elektronicznej

§ 16

1. Bank jest zobowiązany zablokować dostęp do bankowości internetowej, uniemożliwiając tym samym wykonanie transakcji w jednym z następujących przypadków:
 - 1) złożenia przez użytkownika/pasywnego użytkownika dyspozycji zablokowania dostępu do serwisu internetowego;
 - 2) kolejnego trzykrotnego wpisania nieprawidłowego hasła dostępu.
2. Bank ma prawo częściowo ograniczyć lub zablokować dostęp do bankowości internetowej i/lub czasowo zablokować wykonanie dyspozycji w następujących przypadkach:
 - 1) uzasadnionych przyczyn związanych z bezpieczeństwem dostępu do serwisu internetowego i indywidualnych danych uwierzytelniających, w tym w przypadku podejrzenia popełnienia przestępstwa na szkodę użytkownika;
 - 2) umyślnego doprowadzenia do nieautoryzowanej transakcji płatniczej przez użytkownika lub uzasadnionego podejrzenia, że użytkownik będzie posługiwał się dostępem w sposób niezgodny z regulaminem;

- 3) korzystania przez użytkownika z bankowości internetowej niezgodnie z zasadami bezpieczeństwa określonymi w niniejszym załączniku lub w sposób zagrażający bezpieczeństwu korzystania z bankowości internetowej;
 - 4) dokonywania czynności konserwacyjnych bankowości internetowej lub innych systemów teleinformatycznych związanych z wykonywaniem umowy, o czym Bank z wyprzedzeniem poinformuje komunikatem w bankowości lub na stronie internetowej Banku;
 - 5) dokonywania czynności mających na celu usunięcie awarii, usterek lub nieprawidłowości działania bankowości internetowej 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 lub na stronie internetowej Banku;
 - 7) uzasadnionego podejrzenia, iż transakcje na rachunku klienta mają związek z popełnieniem przestępstwa związanego z praniem pieniędzy lub finansowaniem terroryzmu;
 - 8) gdy na rachunku klienta wystąpi zamrożenie wartości majątkowych;
 - 9) braku możliwości zastosowania środków bezpieczeństwa finansowego, w tym brak aktualnego dokumentu tożsamości klienta lub osób upoważnionych do działania w jego imieniu.
3. Bank może uchylić ograniczenie albo blokadę dostępu do bankowości internetowej w przypadku, o którym mowa w ust. 2 pkt 1, na wniosek złożony przez posiadacza rachunku, w sposób określony w ust. 4. W takim przypadku Bank wydaje użytkownikowi/pasywnemu użytkownikowi nowe indywidualne dane uwierzytelniające lub dokona uchylenia ograniczenia lub blokady przy zachowaniu dotychczasowych danych uwierzytelniających.
4. W przypadku, o którym mowa w ust. 2 pkt 1 uchylenie:
- 1) ograniczenia lub blokady dostępu do bankowości internetowej następuje na podstawie telefonicznej lub złożonej w Banku dyspozycji klienta;
 - 2) czasowej blokady dyspozycji następuje po telefonicznym lub pisemnym kontakcie pracownika Banku z klientem i po potwierdzeniu przez klienta złożonej dyspozycji.
5. Z zastrzeżeniem ust. 6, Bank informuje użytkownika o zamiarze zablokowania indywidualnych danych uwierzytelniających w przypadkach określonych w ust. 2 pkt 1 i 3, przed ich zablokowaniem, a jeżeli nie jest to możliwe – niezwłocznie po zablokowaniu telefonicznie.
6. Bank nie przekazuje informacji o zablokowaniu, jeżeli przekazanie tej informacji byłoby nieuzasadnione ze względów bezpieczeństwa lub zabronione na mocy odrębnych przepisów.
7. W przypadkach, o których mowa w ust. 2 pkt 4 i 5 ograniczenie lub blokada dostępu do serwisu internetowego i/lub czasowa blokada dyspozycji następuje przez możliwe krótki okres niezbędny do usunięcia przyczyny ograniczenia lub blokady.

Rozdział 5. Blokowanie i zastrzeżenie dostępu do bankowości internetowej

§ 17

1. Dostęp do serwisu internetowego oraz możliwość posługiwania się indywidualnymi danymi uwierzytelniającymi może zostać zablokowany przez:
 - 1) Bank – zgodnie z postanowieniami § 19;
 - 2) użytkownika/pasywnego użytkownika.
2. Na wniosek posiadacza rachunku Bank może zablokować dostęp do usługi bankowości internetowej uniemożliwiając jednocześnie dokonywanie transakcji przez wszystkich użytkowników.

§ 18

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 pod numerami telefonów wskazanymi i aktualizowanymi przez Bank w formie komunikatu zamieszczonego 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 bankowości internetowej.
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 powiązany z numerem telefonu oznaczonym, jako telefon do autoryzacji lub zmiany numeru telefonu do autoryzacji, użytkownik jest zobowiązany do dokonania zmiany danych osobiście w placówce Banku.
7. Do chwili otrzymania powiadomienia, o którym mowa w ust. 1, Bank nie ponosi odpowiedzialności za informacje uzyskane przez osoby trzecie lub operacje wykonane przez Bank na podstawie dyspozycji złożonych przez te osoby, jeżeli w wyniku nieuprawnionego użycia przez te osoby indywidualnych środków uwierzytelniających, system bankowy zidentyfikował podmiot składający oświadczenie woli, jako uprawniony do złożenia takiego oświadczenia woli zgodnie z umową.
8. Użytkownik/pasywny użytkownik ponosi odpowiedzialność za wszelkie skutki będące następstwem użycia przez osoby nieuprawnione indywidualnych danych uwierzytelniających lub niedopełnienia przez użytkownika/ pasywnego użytkownika obowiązków, o których mowa w niniejszym paragrafie.

§ 19

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. powzięcia informacji o wejściu w ich posiadanie osób nieuprawnionych;
 - 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 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.

§ 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 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 bankowości internetowej zainicjował transakcję płatniczą realizowaną w oparciu o kartę płatniczą na daną kwotę przy użyciu instrumentu płatniczego opartego na tej karcie wydanej przez danego dostawcę, oraz
 - 3) dostawca uwierzytelnia 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 należyście 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. Aplikacja mobilna Nasz Bank

A. Korzystanie z aplikacji mobilnej

§ 21

1. Aplikacja mobilna Nasz Bank udostępniona jest w sklepie Google Play dla systemu Android oraz App Store dla systemu IOS.
2. Po pobraniu i aktywacji aplikacji, użytkownik nadaje PIN do aplikacji oraz określa sposób logowania do aplikacji.
3. Logowanie do aplikacji może odbywać się za pomocą PIN-u do aplikacji lub identyfikacji danymi biometrycznymi.
4. Korzystanie z identyfikacji danymi biometrycznymi wymaga aktywacji tej funkcji na zaufanym urządzeniu mobilnym wraz z rejestracją indywidualnych cech fizycznych, a także aktywacji tej funkcji w aplikacji. Aplikacja nie przetwarza danych biometrycznych użytkownika.
5. Użytkownik może korzystać z aplikacji wyłącznie na zaufanym urządzeniu mobilnym.
6. Po pobraniu i aktywacji aplikacji mobilnej, użytkownik może autoryzować transakcje w aplikacji poprzez zatwierdzenie odpowiedniego komunikatu push (autoryzacja mobilna) lub hasłami SMS. W przypadku posiadania kilku urządzeń, powiadomienia push dotyczące autoryzacji będą wysyłane na wszystkie urządzenia mobilne z aktywną autoryzacją mobilną.
7. Aktywacja autoryzacji mobilnej w aplikacji Nasz Bank na urządzeniu samodzielnie przez użytkownika wymaga podania otrzymanego kodu SMS.
8. W przypadku wyboru autoryzacji transakcji w aplikacji mobilnej Nasz Bank, przywrócenie autoryzacji na hasła SMS użytkownik może dokonać:
 - 1) w placówce Banku,
 - 2) samodzielnie w Internet Banking – podczas wykonywania transakcji w serwisie Internet Banking i pojawienia się komunikatu dotyczącego wysłania powiadomienia autoryzacyjnego na urządzenie mobilne, zostanie wyświetlona możliwość przełączenia na autoryzację SMS; wybór tej opcji skutkuje wysłaniem wiadomości e-mail zawierającej kod do wpisania na stronie, po wprowadzeniu którego zostaną wyświetlone dodatkowe pytania weryfikujące; poprawna weryfikacja odpowiedzi spowoduje zmianę autoryzacji mobilnej na hasła SMS,
 - 3) poprzez rezygnację z aplikacji mobilnej, tj. świadome usunięcie przez klienta urządzenia mobilnego w Internet Bankingu lub usunięcie profilu w aplikacji mobilnej.
9. W przypadku zablokowania użytkownika (tj. 3-krotnego wpisania niewłaściwego e-PIN) lub odinstalowania aplikacji mobilnej Nasz Bank system automatycznie nie zmienia sposobu autoryzacji klienta. Usunięcie ostatniego/jedynego urządzenia z aktywną autoryzacją mobilną spowoduje zmianę sposobu autoryzacji na SMS.
10. Po pobraniu i aktywacji aplikacji mobilnej Nasz Bank użytkownik, ze względów bezpieczeństwa, może mieć ograniczone czasowo niektóre funkcjonalności, np. nie może zmienić limitów transakcji w Internet Banking w ciągu 24 h ani dokonywać wypłat BLIK w bankomacie w ciągu 1h od momentu aktywacji tej aplikacji.
11. Wykonywanie przelewów, generowanie kodu BLIK oraz korzystanie ze smartKARTY w aplikacji mobilnej Nasz Bank możliwe jest wyłącznie na urządzeniach z aktywną autoryzacją mobilną.
12. Dezaktywacja aplikacji na zaufanym urządzeniu mobilnym jest jednoznaczna z odwołaniem przez użytkownika zgody na korzystanie z bankowości mobilnej na tym urządzeniu mobilnym. Usunięcie aplikacji mobilnej z urządzenia mobilnego bez uprzedniej dezaktywacji aplikacji nie jest równoznaczne z odwołaniem zgody na korzystanie z bankowości mobilnej. Sposób dezaktywacji aplikacji mobilnej opisany jest w Przewodnikach po aplikacji.
13. W przypadku nieudanego logowania poprzez identyfikację danymi biometrycznymi wymagane jest logowanie do aplikacji za pomocą PIN-u do aplikacji.
14. Błędne uwierzytelnienie użytkownika podczas logowania do aplikacji polegające na 3-krotnym wprowadzeniu błędnego PIN-u do aplikacji, powoduje automatyczne zablokowanie dostępu do aplikacji.
15. Licznik prób błędnego logowania jest zerowany po poprawnym zalogowaniu się do aplikacji, pod warunkiem, że nie nastąpiło zablokowanie dostępu do aplikacji.
16. Odblokowanie dostępu do aplikacji następuje przez użytkownika poprzez:
17. przeprowadzenie dezaktywacji i ponownej aktywacji aplikacji na zaufanym urządzeniu,
18. w dowolnej placówce Banku przez pracownika Banku.
19. Szczegółowe funkcjonalności oraz zasady korzystania z aplikacji Nasz Bank określają Przewodniki po tej aplikacji.

B. Zasady bezpieczeństwa

§ 22

1. Użytkownik jest zobowiązany do:
 - 1) ochrony identyfikatora, hasła do bankowości internetowej, kodu SMS, PIN-u do aplikacji oraz zaufanego urządzenia mobilnego przed nieuprawnionym przejęciem lub użyciem przez osoby trzecie,
 - 2) niezwłocznego zgłoszenia utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia urządzenia mobilnego, na którym znajduje się aplikacja mobilna,
 - 3) niezwłocznego zgłoszenia nieuprawnionego użycia aplikacji mobilnej, usługi BLIK czy smartKARTY,
 - 4) niezwłocznego zgłoszenia Bankowi nieuprawnionego dostępu do rachunku za pomocą transakcji w ramach BLIK,
 - 5) nieudostępniania aplikacji mobilnej ani kodu BLIK osobom nieuprawnionym,
 - 6) nieudostępniania indywidualnych danych uwierzytelniających, w szczególności kodu autoryzacyjnego oraz jego ochrony,
 - 7) posługiwania się kodem BLIK zgodnie z jego przeznaczeniem,
 - 8) przechowywania PIN-u do aplikacji oraz urządzenia mobilnego, na którym została zainstalowana aplikacja mobilna z zachowaniem należytej staranności.
2. Zgłoszenie utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia urządzenia mobilnego z zainstalowaną aplikacją następuje:
 - 1) w oddziale Banku lub
 - 2) telefonicznie w godzinach pracy Banku.
3. Na podstawie zgłoszenia, o którym mowa ust. 2, Bank zastrzega usługę BLIK/smartKARTĘ lub dostęp do aplikacji mobilnej, co uniemożliwia posługiwanie się daną usługą/aplikacją na zaufanym urządzeniu mobilnym.
4. Zastrzeżenie dokonane jest bezterminowo, powodując brak możliwości dalszego korzystania z usługi/aplikacji.

- Po dokonaniu zastrzeżenia usługi BLIK/usługi smartKARTY użytkownik może ponownie włączyć usługę BLIK/smartKARTA w aplikacji mobilnej, o ile nie nastąpiło zablokowanie dostępu do aplikacji.
- Użytkownik może sam, w każdej chwili, zablokować/odblokować usługę BLIK/usługę smartKARTA w ustawieniach aplikacji poprzez wyłączenie/włączenie tej funkcjonalności.
- Za udostępnienie zaufanego urządzenia mobilnego, udostępnienie aplikacji lub ujawnienie PIN-u do aplikacji osobom trzecim odpowiedzialność ponosi użytkownik aplikacji.
- Użytkownik jest zobowiązany używać aplikacji pochodzącej z wiarygodnego źródła (wyłącznie ze sklepów Google Play oraz App Store).
- Zaleca się, by użytkownik zapewnił ochronę zaufanego urządzenia mobilnego przy pomocy:
 - kodu odblokowującego ekran,
 - programu antywirusowego.
- Nie zaleca się otwierania na zaufanym urządzeniu mobilnym wiadomości e-mail, załączników do e-mail i linków do stron www, pochodzących z nieznanego źródła i od nieznanego osoby.
- 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.
- Nie należy instalować na urządzeniu mobilnym nielegalnych, nieznanego programu, otrzymywanych pocztą e-mail lub pobranych ze stron internetowych.
- Bank nigdy nie wymaga ujawnienia haseł oraz zainstalowania dodatkowego oprogramowania lub certyfikatów.
- Użytkownik nie powinien korzystać z aplikacji mobilnej na urządzeniu mobilnym z usuniętymi fabrycznymi ograniczeniami systemowymi.

C. Ograniczenia w korzystaniu z aplikacji mobilnej

§ 23

- Bank uprawniony jest do czasowego zablokowania usługi BLIK/usługi smartKARTY/aplikacji mobilnej w przypadku:
 - uzasadnionych przyczyn związanych z bezpieczeństwem usługi,
 - stwierdzenia dokonania lub próby dokonania transakcji przez osobę nieuprawnioną,
 - użytkownika usługi w sposób niezgodny z prawem,
 - umyślnego doprowadzenia do nieautoryzowanych transakcji.
- Bank jest zobowiązany zablokować dostęp do aplikacji, uniemożliwiając tym samym wykonanie dyspozycji, w jednym z następujących przypadków:
 - złożenia przez użytkownika dyspozycji zablokowania lub dezaktywacji aplikacji;
 - 3-krotnego wprowadzenia nieprawidłowego PIN-u do aplikacji.
- Bank ma prawo częściowo ograniczyć lub zablokować dostęp do aplikacji i/lub czasowo zablokować wykonanie dyspozycji w następujących przypadkach:
 - uzasadnionych przyczyn związanych z bezpieczeństwem, tj.:
 - uzyskania informacji w tym podejrzenia, iż dyspozycje w aplikacji składane są przez osoby nieuprawnione,
 - zagrożenia przechwycenia danych dostępowych przez złośliwe oprogramowanie,
 - wykorzystywania danych dostępowych przez oprogramowanie automatycznie logujące się z dużą częstotliwością,
 - wykorzystywania systemów lub rachunków w sposób niezgodny z obowiązującymi przepisami prawa,
 - wykonywania działań mogących zagrażać bezpieczeństwu systemu i danych w nim przetwarzanych;
 - podejrzenia nieuprawnionego użycia aplikacji, zaufanego urządzenia mobilnego, indywidualnych danych uwierzytelniających lub umyślnego doprowadzenia do nieautoryzowanej dyspozycji;
 - powzięcia informacji o zagrożeniu bezpieczeństwa dyspozycji;
 - dokonywania czynności konserwacyjnych aplikacji lub innych systemów teleinformatycznych, związanych z korzystaniem z aplikacji, o czym Bank z wyprzedzeniem poinformuje użytkownika w aplikacji mobilnej;
 - dokonywania czynności mających na celu usunięcie awarii, usterek lub nieprawidłowości działania aplikacji lub innych systemów teleinformatycznych związanych z jej obsługą.
- Bank może uchylić ograniczenie albo blokadę dostępu do aplikacji w przypadku, o którym mowa w ust. 3 pkt 1-3, jeżeli na wniosek użytkownika, Bank wyda użytkownikowi nowe indywidualne dane uwierzytelniające.
- W przypadkach, o których mowa w ust. 3 pkt 2-5, ograniczenie lub blokada dostępu do aplikacji i/lub czasowa blokada dyspozycji następuje przez możliwie krótki okres niezbędny do usunięcia przyczyny ograniczenia lub blokady.
- Bank może zablokować dostęp do aplikacji w przypadku wygaśnięcia umów produktowych zawartych przez użytkownika z Bankiem.

§ 24

- Ze względów bezpieczeństwa wykonywania transakcji, Bank ma prawo wprowadzić kwotowe ograniczenia wysokości limitów transakcji wykonywanych w ramach usługi BLIK/usługi smartKARTA.
- Dzienne limity dla transakcji BLIK:

Rodzaj limitu BLIK	wartość standardowa	wartość maksymalna	limit ilościowy
Dzienny limit wypłat gotówki	2.000 PLN	5.000 PLN	10 szt
Dzienny limit transakcji bezgotówkowych w tym dzienny limit transakcji internetowych	5.000 PLN 2.000 PLN	5.000 PLN 5.000 PLN	100 szt 100 szt
Limit pojedynczej transakcji przelew na telefon BLIK	500 PLN	500 PLN	
Dzienny limit wszystkich transakcji przelewów na telefon BLIK	5.000 PLN	5.000 PLN	
Dzienny limit globalny BLIK (przelewy, przelewy na telefon BLIK oraz prośby o przelew BLIK)	5.000 PLN	5.000 PLN	

- Użytkownik może zgłaszać indywidualne limity BLIK, z wyłączeniem limitu globalnego oraz limitów ilościowych.
- Limity dla transakcji w usłudze smartKARTA:

Rodzaj limitu	wartość standardowa
Dzienny limit wypłat gotówki	2.000 PLN
Limit pojedynczej wpłaty gotówki	40.000 PLN
Limit dzienny wpłat gotówki	100.000 PLN
Limit miesięczny wpłat gotówki	500.000 PLN

- Użytkownik może zgłosić wniosek o indywidualne limity w usłudze smartKARTA. W przypadku złożenia przez klienta wniosku o zwiększenie limitu indywidualnego dla wpłat, decyzję podejmuje Dyrektor Oddziału.
- Podczas dokonywania wpłaty w bankomatach recyklingowych Bank może zapytać o źródło pochodzenia wpłacanych środków.

D. BLIK w aplikacji mobilnej

§ 25

- Usługa BLIK to usługa umożliwiająca dokonywanie transakcji BLIK za pomocą aplikacji mobilnej Nasz Bank.
- Bank udostępnia usługę BLIK użytkownikowi bez konieczności składania dodatkowego wniosku. Aktywacja usługi BLIK odbywa się w aplikacji poprzez jej włączenie w ustawieniach.
- Z usługi BLIK może korzystać wyłącznie użytkownik, który pobrał na zaufanym urządzeniu aplikację mobilną Nasz Bank.
- W celu korzystania z usługi BLIK użytkownik powinien łącznie spełnić następujące wymagania:
 - posiadać zaufane urządzenie mobilne,

- 2) posiadać rachunek walucie PLN, w ciężar którego będą realizowane transakcje BLIK,
 - 3) posiadać na urządzeniu mobilnym zainstalowaną aplikację mobilną Nasz Bank,
 - 4) włączyć w ustawieniach aplikacji usługę BLIK,
 - 5) zaakceptować zasady funkcjonowania usługi.
3. Użytkownik jest zobowiązany do korzystania z usługi BLIK w sposób zgodny z obowiązującym prawem, niniejszym regulaminem i przewodnikiem po aplikacji mobilnej Nasz Bank.
4. Użyte definicje mają następujące znaczenie:
- 1) baza powiązań BLIK – baza danych odbiorców przelewów na telefon BLIK prowadzona przez PSP,
 - 2) kod BLIK – 6-cyfrowy kod niezbędny do realizowania transakcji w ramach usługi BLIK, generowany w aplikacji,
 - 3) płatność BLIK – płatności za towary lub usługi w sklepie stacjonarnym/punkcie usługowym lub w sklepie internetowym z wykorzystaniem kodu BLIK, płatność BLIK jest poleceniem przelewu albo poleceniem przelewu wewnętrznego,
 - 4) przelew na telefon BLIK – przelew krajowy, wykonywany na podstawie dyspozycji składanej w aplikacji, polegający na przekazaniu środków pieniężnych na konto odbiorcy zarejestrowanego w bazie powiązań BLIK i realizowany w czasie rzeczywistym w dniu złożenia dyspozycji przelewu, przelew na telefon BLIK jest poleceniem przelewu, użytkownik wykonując przelew podaje numer telefonu komórkowego odbiorcy,
 - 5) prośba o przelew BLIK¹⁴ – przelew krajowy inicjowany przez nadawcę prośby poprzez wysłanie komunikatu zawierającego prośbę o przelew kierowaną do użytkownika (nadawcy przelewu) za pośrednictwem PSP, który może zostać złożony wyłącznie przez użytkownika posiadającego aktywną usługę BLIK. Przelew ten jest wykonywany jedynie z rachunku powiązanego z usługą BLIK. Przelew na prośbę BLIK jest wykonywany na numer rachunku, do którego nadawca prośby jest uprawniony, na podstawie wskazanego w treści prośby numer telefonu. W tym rodzaju przelewu krajowego, unikatowym identyfikatorem jest numer telefonu, który jednoznacznie identyfikuje nadawcę prośby biorącego udział w tej transakcji płatniczej,
 - 6) PSP – Polski Standard Płatności sp. z o.o. z siedzibą w Warszawie, będąca podmiotem zarządzającym i udostępniającym system BLIK,
 - 7) transakcje BLIK – płatności BLIK, wypłaty BLIK i przelewy na telefon BLIK,
 - 8) wypłata BLIK – transakcja BLIK polegająca na wypłacie środków pieniężnych w bankomacie lub w terminalu POS w sklepie stacjonarnym/punkcie usługowym, dokonywana bez użycia karty płatniczej, wypłata BLIK jest wypłatą gotówki.

§ 26

1. W ramach usługi BLIK mogą być realizowane następujące rodzaje transakcji:
 - 1) wypłata gotówki w bankomatach oznaczonych znakiem BLIK,
 - 2) wypłata gotówki w ramach usługi cash back w punktach handlowo – usługowych akceptujących BLIK,
 - 3) płatność za towary i usługi w polskich złotych:
 - a) w terminalach POS u akceptantów oznaczonych znakiem BLIK,
 - b) przez internet u akceptantów oznaczonych znakiem BLIK,
 - 4) wysyłanie przelewów na telefon BLIK,
 - 5) odbieranie przelewów na telefon BLIK,
 - 6) prośba o przelew BLIK¹⁵.
2. Użytkownik może realizować transakcje w ramach usługi BLIK do wysokości salda dostępnego na rachunku i w ramach limitów określonych dla transakcji BLIK.
3. Bank udostępnia informacje o aktualnie obowiązujących limitach BLIK w niniejszym rozdziale.

E. Realizacja transakcji dokonywanych w usłudze BLIK

§ 27

1. Transakcje w usłudze BLIK:
 - 1) mogą być dokonywane w polskich złotych
 - 2) są rozliczane na rachunkach prowadzonych w polskich złotych.
2. Dokonując transakcji w usłudze BLIK, użytkownik zobowiązany jest do jej autoryzacji na zasadach opisanych w ust. 4.
3. Za moment otrzymania przez Bank zlecenia płatniczego dotyczącego transakcji BLIK uznaje się moment dokonania autoryzacji transakcji BLIK przez użytkownika.
4. Użytkownik dokonuje autoryzacji transakcji BLIK – u akceptantów wyposażonych w terminal POS lub umożliwiających dokonanie transakcji BLIK w internecie, wykonując następujące czynności:
 - 1) uruchamia aplikację mobilną z użyciem kodu PIN dla aplikacji lub logowania biometrycznego,
 - 2) generuje kod BLIK w aplikacji mobilnej,
 - 3) wprowadza kod BLIK na terminalu POS lub na stronie internetowej,
 - 4) potwierdza transakcję BLIK w aplikacji mobilnej.
5. Przelew na telefon BLIK zostanie wykonany na numer rachunku, który jest przypisany w bazie powiązań BLIK do numeru telefonu komórkowego podanego przez użytkownika w aplikacji lub systemie bankowym. W celu otrzymywania przelewów na telefon BLIK użytkownik musi dodatkowo dokonać rejestracji w bazie powiązań BLIK, która polega na zapisaniu w niej numeru telefonu komórkowego oraz numeru rachunku, który będzie uznawany kwotą przelewu na telefon BLIK. Od chwili dokonania rejestracji w bazie powiązań BLIK, wszystkie przelewy na telefon BLIK wykonywane na numer telefonu podany w tej bazie są kierowane na rachunek płatniczy podany w bazie powiązań BLIK. Po zmianie numeru telefonu komórkowego użytkownik zarejestrowany w bazie powiązań BLIK w celu dalszego otrzymywania przelewów na telefon BLIK powinien zmienić swoje dane w bazie powiązań BLIK za pośrednictwem aplikacji. Tylko jeden numer telefonu może być powiązany przez użytkownika w bazie powiązań BLIK z numerem rachunku.
6. Prawdłowa dyspozycja przelewu na telefon BLIK, powinna zawierać:
 - 1) numer telefonu komórkowego odbiorcy przelewu;
 - 2) kwotę przelewu wyrażoną w PLN, nie wyższą niż kwota limitu dla tego typu zleceń płatniczych i nie wyższą niż kwota środków na danym rachunku płatnika;
 - 3) dane identyfikujące odbiorcę;
 - 4) tytuł przelewu na telefon BLIK.
7. Dyspozycja przelewu na prośbę BLIK¹⁶ może być złożona przez użytkownika po otrzymaniu w aplikacji mobilnej prośby o przelew od innego użytkownika lub klienta innego banku, który jest uprawniony do rachunku powiązanego z systemem rozliczeń BLIK. Użytkownik zlecający przelew występuje w charakterze płatnika, a przysyłający komunikat zawierający prośbę o przelew – zwany będzie nadawcą.
8. Prawdłowa prośba o przelew BLIK powinna zawierać:
 - 1) kwotę przelewu wyrażoną w PLN;
 - 2) tytuł przelewu;
 - 3) znane nadawcy i zapisane w urządzeniu mobilnym oznaczenie lub imię i nazwisko płatnika i jego numer telefonu powiązany z systemem rozliczeń BLIK. Na podstawie tej prośby Bank wyświetli płatnikowi dodatkowo imię i nazwisko nadawcy powiązane z jego numerem telefonu w banku nadawcy oraz dodatkowo bank może wyświetlić należący do nadawcy numer rachunku BLIK albo inny rachunek powiązany z systemem BLIK, do którego nadawca jest uprawniony.
9. Nadawca może anulować prośbę o przelew BLIK w aplikacji mobilnej najpóźniej przed autoryzacją przelewu przez płatnika. Prośba o przelew BLIK jest ważna 72 godziny od chwili wysłania jej przez nadawcę.

¹⁴ Po udostępnieniu funkcjonalności przez Bank.

¹⁵ Po udostępnieniu funkcjonalności przez Bank.

¹⁶ Po udostępnieniu funkcjonalności przez Bank.

10. Bank umożliwia wysłanie więcej niż jednej prośby o przelew BLIK. Ze względów bezpieczeństwa Bank może jednak ograniczyć liczbę jednorazowo wysyłanych próśb o przelew.
11. Użytkownik może całkowicie wyłączyć możliwość odbierania próśb o przelew BLIK albo zablokować możliwość otrzymywania próśb o przelew BLIK od innego wskazanego użytkownika i określonego numeru telefonu. Blokada może być wycofana przez użytkownika.
12. Po otrzymaniu prośby o przelew BLIK płatnik może ją odrzucić albo zlecić przelew. Złożenie dyspozycji przelewu na prośbę BLIK następuje na wskazany w jej treści numer telefonu powiązany z nadawcą, na kwotę oraz tytuł wskazane przez nadawcę w treści komunikatu zawierającego prośbę o przelew.
13. Korzystanie z usługi BLIK wymaga:
 - 1) dla transakcji BLIK – wybrania rachunku, który będzie obciążany i uznawany kwotą transakcji BLIK,
 - 2) dla odbierania/wysyłania przelewów na telefon BLIK – rejestracji numeru telefonu komórkowego w bazie powiązań BLIK, który inni klienci mogą podawać jako unikatowy identyfikator w dyspozycjach przelewów na telefon BLIK w Banku,
 - 3) dla realizacji próśb o przelew BLIK – posiadania aktywnej usługi BLIK oraz rejestracji numeru telefonu komórkowego w bazie powiązań BLIK.
14. Użytkownik ma możliwość zmiany parametrów, o których mowa w ust. 13, w aplikacji mobilnej Nasz Bank. Zmiana potwierdzana jest PIN-em do aplikacji.
15. Bank realizuje transakcje BLIK:
 - 1) przez całą dobę,
 - 2) w dniu jej otrzymania.
16. Bank odmawia przyjęcia realizacji transakcji BLIK w przypadku, gdy:
 - 1) rachunek wskazany do usługi BLIK został zamknięty,
 - 2) użytkownik podał nieprawidłowe dane podczas autoryzacji transakcji BLIK,
 - 3) użytkownik przekroczył czas, wskazany w aplikacji mobilnej, w którym powinien dokonać zatwierdzenia transakcji,
 - 4) przekroczony został czas ważności kodu BLIK,
 - 5) kwota transakcji jest wyższa od limitu BLIK,
 - 6) kwota transakcji jest wyższa od środków dostępnych na rachunku.
17. Akceptant ma prawo odmówić przyjęcia transakcji BLIK w przypadku, gdy:
 - 1) użytkownik podał nieprawidłowe dane podczas autoryzacji transakcji,
 - 2) nie można uzyskać zgody Banku na realizację transakcji BLIK.
18. Anulowanie transakcji BLIK możliwe jest do momentu dokonania przez użytkownika autoryzacji transakcji BLIK; po dokonaniu autoryzacji transakcji BLIK użytkownik może anulować transakcję BLIK wyłącznie u akceptanta, o ile akceptant oferuje taką możliwość.

§ 28

1. Wykorzystywany podczas autoryzacji kod BLIK:
 - 1) jest kodem jednorazowym ważnym maksymalnie 120 sekund od momentu jego wygenerowania, a informacja o zbliżającym się upływie czasu jego ważności jest podawana w aplikacji mobilnej Nasz Bank,
 - 2) wygasa z upływem czasu jego ważności lub z chwilą autoryzacji transakcji BLIK, do której został wygenerowany.
2. Przelewy na telefon BLIK wychodzące z Banku są realizowane jako:
 - 3) przelewy wewnętrzne – w sytuacji, gdy rachunek odbiorcy jest rachunkiem prowadzonym w Banku,
 - 4) przelewy Express Elixir – w sytuacji, gdy rachunek odbiorcy nie jest rachunkiem prowadzonym w Banku.
3. Dyspozycje składane w aplikacji przez użytkownika wymagają autoryzacji z użyciem indywidualnych danych uwierzytelniających:
 - 1) PIN-u do aplikacji lub
 - 2) identyfikacji danymi biometrycznymi,
4. Autoryzacja zlecenia płatniczego BLIK przez użytkownika oznacza jego zgodę na wykonanie transakcji płatniczej. Cofnięcie zgody od chwili autoryzacji nie jest możliwe.

F. Usługa smartKARTA w aplikacji mobilnej Nasz Bank

§ 29

1. Usługa smartKARTA to usługa umożliwiająca dokonywanie transakcji w bankomacie/bankomacie recyklingowym Banku przy pomocy wygenerowanego w aplikacji mobilnej Nasz Bank kodu QR, bez dotykania urządzenia.
2. Bank udostępni usługę smartKARTA użytkownikowi bez konieczności składania dodatkowego wniosku. Aktywacja usługi odbywa się w aplikacji poprzez włączenie jej w ustawieniach.
3. Z usługi smartKARTA może korzystać wyłącznie użytkownik, który pobrał na zaufanym urządzeniu aplikację mobilną Nasz Bank.
4. W celu korzystania z usługi smartKARTA użytkownik powinien łącznie spełnić następujące wymagania:
 - 1) posiadać zaufane urządzenie mobilne,
 - 2) posiadać rachunek walucie PLN, w ciężar którego będą realizowane transakcje,
 - 3) posiadać na urządzeniu mobilnym zainstalowaną aplikację mobilną Nasz Bank.
5. Użytkownik jest zobowiązany do korzystania z usługi smartKARTA w sposób zgodny z obowiązującym prawem, niniejszym regulaminem i *Przewodnikiem po aplikacji mobilnej*.

§ 30

1. W ramach usługi smartKARTA mogą być realizowane następujące rodzaje transakcji:
 - 1) wypłata gotówki w bankomatach własnych Banku,
 - 2) wpłata gotówki w bankomatach recyklingowych Banku. Wykaz bankomatów recyklingowych obsługujących wpłatę gotówki znajduje się na stronie internetowej Banku: www.bszl.com.pl.
2. Użytkownik może realizować transakcje w ramach usługi smartKARTA do wysokości salda dostępnego na rachunku i w ramach limitów określonych dla transakcji w usłudze smartKARTA.

G. Realizacja transakcji dokonywanych w usłudze smartKARTA

§ 31

1. Transakcje w usłudze smartKARTA:
 - 1) mogą być dokonywane w polskich złotych,
 - 2) są rozliczane na rachunkach prowadzonych w polskich złotych.
2. Dokonując transakcji w usłudze smartKARTA, użytkownik zobowiązany jest do jej autoryzacji na zasadach opisanych w ust. 4.
3. Za moment otrzymania przez Bank zlecenia płatniczego dotyczącego transakcji w usłudze smartKARTA uznaje się moment dokonania autoryzacji transakcji w usłudze smartKARTA przez użytkownika.
4. Użytkownik dokonuje autoryzacji transakcji w usłudze smartKARTA w bankomatach/bankomatach recyklingowych Banku, w następujący sposób:
 - 1) uruchamia aplikację mobilną Nasz Bank z użyciem kodu PIN dla aplikacji lub logowania biometrycznego,
 - 2) wybiera w aplikacji właściwą funkcję (wpłata/wypłata) wraz z kwotą transakcji,
 - 3) skanuje kod QR wyświetlony w bankomacie/bankomacie recyklingowym,
 - 4) potwierdza transakcję w aplikacji mobilnej Nasz Bank.
5. Bank realizuje transakcje w usłudze smartKARTA:
 - 1) przez całą dobę,
 - 2) w dniu jej otrzymania.
6. Bank odmawia przyjęcia realizacji transakcji w usłudze smartKARTA w przypadku, gdy:
 - 1) użytkownik podał nieprawidłowe dane podczas autoryzacji transakcji,

- 2) użytkownik przekroczył czas, wskazany w aplikacji mobilnej, w którym powinien dokonać zatwierdzenia transakcji,
 - 3) kwota transakcji jest wyższa od limitu w usłudze smartKARTA,
 - 4) kwota transakcji jest wyższa od środków dostępnych na rachunku.
7. Anulowanie transakcji smartKARTA możliwe jest do momentu dokonania przez użytkownika autoryzacji transakcji. Po dokonaniu autoryzacji użytkownik nie może anulować transakcji.

H. Funkcjonalności dostępne w aplikacji mobilnej Nasz Bank

§ 32

1. Szczegółowe funkcjonalności dostępne w aplikacji mobilnej Nasz Bank przedstawia tabela:

Funkcjonalność	Dostępność		Informacje dodatkowe
	IB	IBF	
1. Podgląd			
1) lista rachunków (rachunek bieżący, lokata, kredyt)	tak	tak	
2) historia, saldo i dostępne środki	tak	tak	
3) szczegóły rachunku	tak	tak	
4) karty płatnicze	tak	tak	
5) blokady transakcji kartą płatniczą	tak	tak	
2. Przelewy			
1) przelew własny	tak	tak	
2) przelew krajowy	tak	tak	
3) przelew US/ZUS	tak	tak	
4) przelew dewizowy europejski	tak	tak	wyłącznie przelew w walucie EUR
5) doładowanie telefonu	tak	tak	
6) przelew QR	tak	tak	
3. Lokaty			
1) podgląd	tak	tak	
2) założenie lokaty	nie	nie	
3) likwidacja lokaty	nie	nie	
4. Kredyty			
1) podgląd	tak	tak	
2) wniosek o kredyt	nie	nie	
3) spłata kredytu	nie	nie	
5. Usługi kartowe			
1) nadanie/zmiana PINu do karty płatniczej	tak	tak	
2) zmiana statusu karty płatniczej			
a) aktywacja	tak	tak	
b) zablokowanie	tak	tak	
c) odblokowanie	tak	tak	
d) zastrzeżenie	tak	tak	
3) zmiana limitów	tak	tak	pod warunkiem, że użytkownik karty ma do tego prawo
4) włączenie/wyłączenie płatności zbliżeniowych	tak	tak	
5) zamówienie karty płatniczej	nie	nie	
6. Pozostałe usługi			
1) smartKARTA	tak	tak	wykaz bankomatów obsługujących wpłaty i wypłaty za pomocą smartKARTY na stronie: www.bszl.com.pl
2) transakcja przy użyciu kodu BLIK	tak	tak	BLIK w IBF w wariantcie wieloosobowej autoryzacji transakcji – po udostępnieniu przez Bank na wniosek klienta
3) przelew BLIK na numer telefonu	tak	tak	
4) mobilna autoryzacja operacji dokonywanych w IB	tak	tak	
5) mobilna autoryzacja operacji dokonywanych w placówce Banku	tak	tak	możliwe do zatwierdzenia wpłaty i wypłaty kasowe oraz przelewy
6) potwierdzenie transakcji internetowej dokonanej kartą płatniczą z wykorzystaniem usługi 3D Secure	tak	nie	
7) wysłanie wiadomości do Banku	tak	tak	
8) mobilne potwierdzenie tożsamości pracownika Banku	tak	tak	
9) platforma Kantor SGB	tak	tak	
7. Ustawienia			
1) włączenie/wyłączenie BLIKa	tak	tak	
2) zmiana limitów BLIK	nie	nie	
3) rejestracja numeru telefonu w usłudze przelew BLIK na telefon	tak	tak	
4) zmiana limitu wypłaty dla smartKARTY	nie	nie	
5) zmiana PINu do aplikacji	tak	tak	
6) wybór informacji widocznych przed zalogowaniem	tak	tak	
7) wybór metody logowania do aplikacji	tak	tak	
8) zablokowanie kanału dostępu	tak	tak	
8. Inne funkcjonalności, nie wykazane w niniejszej tabeli, zostały opisane w przewodniku po aplikacji mobilnej Nasz Bank.			

2. Pracownik Banku może wysłać użytkownikowi aplikacji mobilnej Nasz Bank komunikat push w formie powiadomienia (informacji) lub żądania autoryzacji.
3. Komunikat, o którym mowa w ust. 2, może służyć m.in. do:
 - 5) poinformowania użytkownika o planowanym kontakcie pracownika Banku z klientem – pracownik Banku, uprzedzając kontakt telefoniczny z klientem, wysyła użytkownikowi aplikacji mobilnej Nasz Bank komunikat push informujący o planowanym kontakcie Banku podając szczegółowe informacje (imię i nazwisko pracownika, dane placówki Banku, datę planowanego kontaktu, cel rozmowy);
 - 6) wyrażenia/niewyrażenia zgody na kontakt pracownika Banku z klientem – pracownik Banku wysyła informacje, o których mowa w punkcie 1, oraz dodatkowo prosi o potwierdzenie bądź odrzucenie komunikatu;

- 7) potwierdzenia tożsamości pracownika Banku w przypadku kontaktu pracownika z klientem – podczas rozmowy telefonicznej z klientem pracownik Banku wysyła komunikat push ze swoimi danymi;
- 8) potwierdzenia tożsamości użytkownika aplikacji w przypadku kontaktu klienta z Bankiem – w celu weryfikacji danych klienta, pracownik Banku wysyła komunikat z prośbą o potwierdzenie danych użytkownika w aplikacji.

Rozdział 8. Standardowe limity pojedynczej transakcji oraz limity wszystkich transakcji w ciągu dnia

§ 33

1. Standardowe maksymalne limity pojedynczej transakcji oraz limity wszystkich transakcji w ciągu dnia dokonywanych za pośrednictwem bankowości elektronicznej:

Limity w Internet Banking – IB			
Kanał dostępu		Limit pojedynczej transakcji	Limit wszystkich transakcji w ciągu dnia
Limity do rachunku w walucie PLN			
Aplikacja mobilna		1 000,00 zł (istnieje możliwość zwiększenia limitu za pośrednictwem IB do 3 000,00 zł na 10 min.)	3 000,00 zł
Serwis internetowy	Płatności ekspresowe BlueCash	5 000,00 zł	5 szt. (łącznie w IB i w Banku)
	Płatności ekspresowe Express Elixir	5 000,00 zł	5 szt. (łącznie w IB i w Banku)
	Przelew standardowy	20 000,00 zł (w przypadku posiadania niższego limitu istnieje możliwość zwiększenia limitu za pośrednictwem IB do 20 000,00 zł na 10 min.)	100 000,00 zł
	Łączny limit IB:	20 000,00 zł	100 000,00 zł
Limity do rachunku w walucie wymiennej EUR/USD/GBP			
Serwis internetowy (IB)		10 000,00 EUR/USD/GBP	20 000,00 EUR/USD/GBP
Aplikacja mobilna		5 000,00 EUR/USD/GBP	10 000,00 EUR/USD/GBP

Limity w Internet Banking – IBF			
Kanał dostępu		Limit pojedynczej transakcji	Limit wszystkich transakcji w ciągu dnia
Limity do rachunku w walucie PLN			
Aplikacja mobilna		autoryzacja przelewów: do wysokości limitu w IB wprowadzanie przelewów: 1 000,00 zł	autoryzacja przelewów: do wysokości limitu w IB wprowadzanie przelewów: 3 000,00 zł
Serwis internetowy	Płatności ekspresowe BlueCash	5 000,00 zł	5 szt. (łącznie w IB i w Banku)
	Płatności ekspresowe Express Elixir	5 000,00 zł	5 szt. (łącznie w IB i w Banku)
	Przelew standardowy	20 000,00 zł (w przypadku posiadania niższego limitu istnieje możliwość zwiększenia limitu za pośrednictwem IBF do 20 000,00 zł na 10 min.)	100 000,00 zł
	Łączny limit IBF:	20 000,00 zł	100 000,00 zł
Limity do rachunku w walucie wymiennej EUR/USD/GBP			
Serwis internetowy (IB)		10 000,00 EUR/USD/GBP	20 000,00 EUR/USD/GBP
Aplikacja mobilna		5 000,00 EUR/USD/GBP	10 000,00 EUR/USD/GBP

2. Limity dotyczą operacji na rachunku.
3. Z zastrzeżeniem ust. 4, Posiadacz rachunku może wnioskować o indywidualne ustalenie limitów, o których mowa w ust. 1.
4. O wysokości limitów ostatecznie decyduje Bank.
5. Przelewy wewnętrzne pomiędzy rachunkami klienta nie są wliczane do limitów, o których mowa w ust. 1.

Rozdział 9. Inne postanowienia

§ 34

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

** po udostępnieniu funkcjonalności w Banku*