

Wyciąg z „Regulaminu kont 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”



(aktualizacja 06.07.2026 r.)

Załącznik nr 3

do „Regulaminu kont dla klientów indywidualnych w Banku Spółdzielczym Ziemi Łowickiej w Łowiczu” – Elektroniczne kanały dostępu

A. Udostępnienie elektronicznych kanałów

§ 1

1. Nasze produkty i usługi udostępniamy przez elektroniczne kanały dostępu:
 - 1) bankowości elektroniczną – zapewniamy dostęp do informacji o naszych produktach i usługach oraz umożliwiamy składanie dyspozycji przez:
 - a) bankowość internetową (serwis internetowy) – korzystasz z niej na komputerze lub urządzeniu mobilnym przez przeglądarkę internetową w wersji na komputer,
 - b) interfejs mobilny – korzystasz z niego na zaufanym urządzeniu mobilnym przez przeglądarkę internetową, interfejs mobilny będzie wyłączony, o całkowitym wyłączeniu poinformujemy Cię na naszej stronie internetowej,
 - c) bankowość mobilną – korzystasz z niej na zaufanym urządzeniu mobilnym, w aplikacji mobilnej Nasz Bank lub SGB Mobile, a jeśli jesteś osobą małoletnią przez aplikację Nasz Bank Junior,
 - 2) usługę SMS Banking – wysyłamy Ci SMS-y z informacjami o transakcjach na Twoim rachunku. Wiadomości wysyłamy codziennie w godz. 6:00-22:00.
2. Bankowość internetową udostępniamy w dwóch wariantach:
 - 1) Internet Banking (IB) – dla użytkowników, którzy samodzielnie zatwierdzają dyspozycje;
 - 2) Internet Banking dla Firm (IBF) – dla rad rodziców i SKO z możliwością jedno lub wieloosobowego zatwierdzania dyspozycji.
3. Za pomocą tego samego loginu wydanego w naszym banku możesz korzystać w serwisie internetowym.
4. Wykaz produktów i usług dostępnych w elektronicznych kanałach dostępu oraz warunki korzystania z usług określają przewodniki dla klientów. Znajdziesz je na naszej stronie internetowej. Otrzymasz je również na swoje życzenie w naszej placówce. Przewodniki dla klienta to instrukcje użytkowania, które zawierają opisy poszczególnych elektronicznych kanałów dostępu, ich wymagania techniczne i zasady prawidłowej obsługi.
5. Informacje o naszych produktach i usługach dostępnych online znajdziesz na naszej stronie internetowej.
6. Informacje o aktualnej ofercie usług dostępnych w aplikacji mobilnej:
 - 1) Nasz Bank oraz Nasz bank Junior znajdują się w niniejszym załączniku do regulaminu oraz w przewodnikach dla klientów po tych aplikacjach,
 - 2) SGB Mobile znajdują się w Regulaminie korzystania z aplikacji mobilnej SGB Mobile, dostępnym na naszej stronie internetowej.

§ 2

1. Aby korzystać z elektronicznych kanałów dostępu, musisz mieć jeden z poniższych rachunków:
 - 1) oszczędnościowy,
 - 2) oszczędnościowo-rozliczeniowy (w tym podstawowy rachunek płatniczy),

- 3) oszczędnościowy w walucie w walucie wymiennej (walutowy) – pod warunkiem, że masz też rachunek oszczędnościowo-rozliczeniowy w walucie PLN, z którego będą pobierane prowizje i opłaty.
2. Na Twoje życzenie możemy udostępnić w bankowości internetowej także lokaty, kredyty oraz inne rachunki, o ile masz już uruchomioną bankowość internetową. Szczegółowy opis funkcji dostępnych dla lokat i kredytów znajdziesz w przewodnikach dla klientów.
3. Aby korzystać z elektronicznych kanałów dostępu, musisz być posiadaczem, współposiadaczem rachunku lub pełnomocnikiem, który ma odpowiednie pełnomocnictwo. Małoletni korzystają z elektronicznych kanałów dostępu na podstawie zgody przedstawiciela ustawowego, w ramach zawartej z nami umowy.
4. Możesz wnioskować o udostępnienie kolejnych produktów lub usług, zmianę warunków świadczenia tych produktów lub usług i zawierać umowy przez elektroniczne kanały dostępu, jeśli udostępniliśmy taki sposób zawierania umów. Informacje o ofercie znajdują się na naszej stronie internetowej. Informacje o sposobach zawierania umów określa regulamin.
5. Jeśli podpisałeś umowę w placówce Banku, możesz otworzyć w bankowości internetowej rachunek oszczędnościowy w złotych lub w walucie wymiennej – o ile udostępniliśmy taką funkcjonalność.
6. Udostępniamy Ci kantor. Zasady, na których świadczymy tę usługę w bankowości elektronicznej, są załącznikiem nr 4.

§ 3

1. Dostęp do bankowości elektronicznej uzyskujesz za pomocą indywidualnych danych uwierzytelniających.
2. Możemy umożliwić Ci korzystanie z usługi przy użyciu tych samych indywidualnych danych uwierzytelniających, jeśli jesteś równocześnie posiadaczem lub pełnomocnikiem do rachunku innego klienta. Uwzględniamy przy tym limity transakcji do rachunku.

§ 4

1. Kiedy wykonujesz transakcje:
 - 1) korzystaj z zaufanych komputerów z aktualnym oprogramowaniem antywirusowym;
 - 2) sprawdź, czy transmisja jest szyfrowana protokołem SSL (ang. Secure Socket Layer), który zapewnia poufność i integralność transmisji danych;
 - 3) nie korzystaj z otwartych i niezabezpieczonych sieci.
2. W przewodnikach dla klienta oraz na naszej stronie internetowej znajduje się szczegółowy opis środków bezpieczeństwa, które powinieneś(-naś) przedsięwziąć, aby bezpiecznie korzystać z elektronicznych kanałów dostępu.
3. Żeby korzystać z usługi, musisz zaakceptować pliki cookies w przeglądarce internetowej. Są one konieczne, aby utrzymać aktywną sesję po zalogowaniu się do bankowości elektronicznej. Szczegółowe informacje o wszystkich rodzajach naszych plików cookies oraz celu ich wykorzystywania znajdują się na naszej stronie internetowej.

§ 5

1. Musisz korzystać z elektronicznych kanałów dostępu zgodnie z umową, regulaminem i przewodnikami dla klientów. Musisz zabezpieczyć otrzymane indywidualne dane uwierzytelniające przed dostępem osób trzecich i zapewnić ich poufność.
2. Gdy otrzymasz indywidualne dane uwierzytelniające z ust. 1, chroń je przed naruszeniem. Ze względów bezpieczeństwa nie przechowuj poszczególnych danych razem ze sobą.
3. Zapewniamy Ci należyłą ochronę indywidualnych danych uwierzytelniających. Są one dostępne wyłącznie dla użytkownika uprawnionego do korzystania z nich.

§ 6

1. Zakres usług możemy zmienić tylko zgodnie z warunkami i trybem przewidzianymi dla zmiany regulaminu.
2. Jeśli wyrazisz zgodę, możemy użyć metody Device Fingerprinting (DFP). Pozwala nam ona rozpoznać Twoje urządzenie, z którego się logujesz. Dzięki temu możemy oznaczyć je jako zaufane. Gdy później

- zalogujesz się z tego samego urządzenia, nie będziesz musiał używać silnego uwierzytelnienia (np. kodu SMS lub aplikacji mobilnej).
3. Urządzenie, które oznaczasz jako zaufane, powinno być używane tylko przez Ciebie.
 4. Więcej informacji o metodzie DFP znajdziesz w przewodniku po bankowości dla klienta.

B. Dyspozycje składane elektronicznie

§ 7

Wszelkie oświadczenia woli, które składasz nam w postaci elektronicznej, będą ważne i prawnie wiążące, jeżeli poprawnie zidentyfikujesz się indywidualnymi danymi uwierzytelniającymi i zastosujesz metody uwierzytelnienia, których wymagamy.

§ 8

1. Do korzystania z rachunków przez elektroniczne kanały dostępu stosuje się te same zasady, które obowiązują przy zwykłym dysponowaniu rachunkiem. Są one opisane w:
 - 1) rozdziale 2 regulaminu – wskazującym, kto i w jaki sposób może dysponować pieniędzmi,
 - 2) rozdziale 4 regulaminu – dotyczącym poszczególnych rodzajów rachunków,z uwzględnieniem § 9-12 tego załącznika.
2. W elektronicznych kanałach dostępu możesz:
 - 1) sprawdzać informacje o swoich rachunkach, w tym saldo, historię,
 - 2) zlecać dyspozycje i transakcje, w tym przelewy krajowe i zagraniczne, przelewy natychmiastowe,
 - 3) zarządzać kartami,
 - 4) składać wnioski, np. o wypłatę świadczenia wychowawczego z programu Rodzina 800+ wraz z załącznikami oraz Dobry start; dostępność usługi zależy od współpracy z Ministerstwem Rodziny i Polityki Społecznej,
 - 5) wymieniać waluty w kantorze,
 - 6) składać inne wnioski, które udostępniamy, dotyczące produktów lub usług podmiotów trzecich współpracujących z nami.Szczegółowy zakres i sposób posługiwania się danym elektronicznym kanałem dostępu opisują przewodniki dla klientów.
3. Świadczymy usługę oferowaną przez integratorów płatności internetowych, którzy inicjują płatności w formie przelewów typu pay by link we współpracy z nami, przy czym:
 - 1) integratorem płatności internetowych jest podmiot, który świadczy usługi sklepom internetowym lub innym podmiotom prowadzącym sprzedaż towarów lub usług; usługi te polegają na umożliwieniu im przyjmowania płatności od ich klientów za pomocą przelewów typu pay by link,
 - 2) przelew typu pay by link realizuje klient, który płaci za zakupy w sklepach internetowych lub u innych podmiotów prowadzących sprzedaż towarów lub usług za pośrednictwem integratorów płatności internetowych.
4. Możesz zgodzić się na transakcję również za pośrednictwem dostawcy, który świadczy usługę inicjowania transakcji płatniczej.
5. Nie możesz odwołać zlecenia płatniczego, jeśli zgodzisz się, aby dostawca świadczący usługę inicjowania transakcji zainicjował transakcję albo ją wykonał. Zasada ta dotyczy inicjowania transakcji przez dostawcę świadczącego usługę inicjowania transakcji lub przez odbiorcę lub za jego pośrednictwem.

§ 9

1. Aby złożyć elektronicznie dyspozycję lub zlecenie płatnicze, musisz się uwierzytelnić w sposób, który pozwoli nam Cię zidentyfikować i zapoznać się z treścią dyspozycji. Dyspozycje te spełniają wymagania formy pisemnej w zakresie, w jakim mają związek z czynnościami bankowymi. Wybrane dyspozycje, które składa małoletni poniżej 13 roku życia, realizujemy, gdy w bankowości mobilnej zatwierdzi je przedstawiciel ustawowy.
2. Gdy złożysz dyspozycję lub zlecenie płatnicze w bankowości elektronicznej, musisz je autoryzować indywidualnymi danymi uwierzytelniającymi, stosując metody uwierzytelniania, których wymagamy.

3. Stosujemy silne uwierzytelnianie, gdy:
- 1) uzyskujesz dostęp do swojego rachunku w trybie online,
 - 2) inicjujesz transakcję płatniczą,
 - 3) przeprowadzasz w kanale zdalnym czynność, która może wiązać się z ryzykiem oszustwa lub innych nadużyć,
- z wyjątkiem sytuacji niewymagających silnego uwierzytelnienia, które wskazujemy w ust. 4.
4. Możemy nie stosować silnego uwierzytelniania, gdy:
- 1) korzystasz z jednej z wymienionych niżej pozycji w trybie online lub z 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 wyjątkiem ust. 5,
 - 2) inicjujesz transakcję do odbiorcy z listy zaufanych odbiorców, którą utworzyłeś(-aś) wcześniej, stosując silne uwierzytelnianie,
 - 3) inicjujesz kolejną transakcję z serii transakcji cyklicznych, na tę samą kwotę, dla tego samego odbiorcy pod warunkiem, że pierwszą transakcję cykliczną utworzyłeś(-aś), zmieniłeś(-aś) lub zainicjowałeś(-eś), stosując silne uwierzytelnienie,
 - 4) inicjujesz transakcję płatniczą w sytuacji, gdy płatnik i odbiorca są tą samą osobą fizyczną lub prawną i prowadzimy oba rachunki płatnicze,
 - 5) inicjujesz transakcję płatniczą, której poziom ryzyka uznajemy za niską, zgodnie z mechanizmem monitorowania naszych transakcji.
5. Stosujemy silne uwierzytelnianie, jeżeli:
- 1) po raz pierwszy uzyskujesz dostęp do informacji z ust. 4 pkt 1 lit. a w trybie online;
 - 2) minęło więcej niż 90 dni, odkąd po raz ostatni uzyskałeś(-aś) dostęp do informacji z ust. 4 pkt 1 lit. b w trybie online oraz odkąd ostatni raz zastosowałeś(-aś) silne uwierzytelnianie.
6. Możemy skontaktować się z Tobą, aby zrealizować zlecenie płatnicze.
7. Aby zalogować się do serwisu internetowego, musisz podać swój identyfikator (login) oraz udostępnione Ci indywidualne dane uwierzytelniające, opisane w ust. 8.
8. Aby uzyskać dostęp do dyspozycji składanych przez serwis internetowy i móc je autoryzować, musisz zalogować się do serwisu internetowego (loginem), a następnie autoryzować operacje używając indywidualnych danych uwierzytelniających:
- 1) dla Internet Bankingu:
 - a) hasła stałego,
 - b) kodu SMS,
 - c) kodu uwierzytelniającego,
 - d) mObywatela (gdy wdrożymy taką funkcjonalność),
 - e) klucza bezpieczeństwa U2F,
 - f) aplikacji mobilnej Nasz Bank lub SGB Mobile i PIN-u do tych aplikacji lub biometrii; wymogi oraz zasady instalacji aplikacji na urządzeniu mobilnym i sposób ich aktywacji opisują przewodniki dla klientów,
 - 2) dla Internet Bankingu dla Firm:
 - a) hasła stałego,
 - b) kodu SMS,
 - c) kodu uwierzytelniającego,
 - d) mObywatela (gdy wdrożymy taką funkcjonalność),
 - e) klucza bezpieczeństwa U2F,
 - f) aplikacji mobilnej Nasz Bank lub SGB Mobile i PIN-u do tych aplikacji lub biometrii; wymogi oraz zasady instalacji aplikacji na urządzeniu mobilnym i sposób ich aktywacji opisują przewodniki dla klientów.

Możemy udostępnić również inne indywidualne dane uwierzytelniające, które opiszemy w przewodnikach dla klientów.

9. Hasło stałe z ust. 8 nadajesz po tym, gdy prześlemy Ci hasło tymczasowe. Nastąpi to podczas pierwszego logowania lub odblokowywania dostępu do bankowości internetowej. Zasady tworzenia hasła stałego (jego składniki) określa przewodnik dla klienta.
10. Umożliwiamy również logowanie do bankowości internetowej za pomocą aplikacji mObywatel (gdy wdrożymy taką funkcjonalność) lub klucza bezpieczeństwa U2F. Sposób rejestracji klucza U2F w bankowości oraz sposób logowania powyższymi metodami opisujemy w przewodnikach dla klientów.
11. Listę aktywnych kluczy bezpieczeństwa U2F możesz modyfikować przez dodanie lub usunięcie poszczególnych kluczy z listy kluczy dostępnej w Twojej bankowości.
12. Podczas logowania się do bankowości internetowej możesz dodać urządzenie, z którego się logujesz, jako urządzenie zaufane. Wtedy kolejne logowania z tego urządzenia do bankowości internetowej w przeglądarce będziesz przeprowadzać już bez dodatkowego uwierzytelnienia za pomocą kodów SMS czy aplikacji mobilnej. Urządzeniem zaufanym może być np. prywatny komputer, smartfon lub tablet, z którego korzystasz wyłącznie Ty. Podczas logowania weryfikujemy określone cechy tego urządzenia.
13. W dowolnym momencie możesz przez bankowość internetową usunąć swoje urządzenie zaufane. Wtedy każde kolejne logowanie do bankowości internetowej będzie wymagało dodatkowego potwierdzania za pomocą kodów SMS lub aplikacji mobilnej.
14. Autoryzacja, którą wykonujesz, oznacza, że polecasz nam wykonać określoną czynność i jest to podstawą jej wykonania.
15. Kody SMS przesyłamy na numer telefonu komórkowego, który podałeś(-aś) nam w banku.
16. Możemy wprowadzić, wycofać oraz zmienić rodzaj stosowanych indywidualnych danych uwierzytelniających. W takim przypadku udostępniamy Ci je oraz zawiadamiamy Cię o zmianie. Informację o stosowanych rodzajach indywidualnych danych uwierzytelniających zamieszczamy w przewodnikach dla klienta.
17. Jeśli podałeś nam e-mail oraz telefon komórkowy możesz samodzielnie zmienić hasło do swojej bankowości. Szczegóły przeczytasz w przewodnikach dla klienta.

§ 10

Moment zarejestrowania odpowiednich danych w bankowości elektronicznej i przyjęcia tego oświadczenia przez nasz serwer uznajemy za chwilę, w której składasz oświadczenie w postaci elektronicznej, w szczególności dyspozycję, lub wykonujesz jakąkolwiek czynność. Od tej zasady mogą obowiązywać wyjątki, które określa umowa, regulamin lub obowiązujące przepisy prawa.

§ 11

1. Dyspozycje, które składasz przez bankowość elektroniczną, realizujemy elektronicznie. Stosujesz zasady autoryzacji obowiązujące dla tego elektronicznego kanału dostępu.
2. Autoryzowanego zlecenia płatniczego nie możesz odwołać, z wyjątkiem sytuacji z § 27 ust. 5 regulaminu.

§ 12

1. To, że przyjęliśmy do realizacji dyspozycję, którą złożyłeś(-aś) przez elektroniczne kanały dostępu, potwierdzamy przez ten sam kanał.
2. Jeśli nie przyjęliśmy dyspozycji, którą złożyłeś(-aś) przez elektroniczny kanał dostępu, powiadomimy Cię o tym oraz o przyczynie odmowy przez ten sam kanał lub pracownika naszej placówki. Możliwe powody:
 - 1) niekompletność dyspozycji,
 - 2) złożenie dyspozycji sprzecznych ze sobą,
 - 3) nieprawidłowy numer rachunku odbiorcy,
 - 4) brak środków do realizacji dyspozycji lub
 - 5) inne okoliczności, które uniemożliwiają nam przyjęcie dyspozycji.

§ 12a

1. W Internet Bankingu dla Firm udostępniamy usługę autowypłaty. Dzięki niej możesz zlecić wypłatę gotówki w naszej placówce dla dowolnej osoby fizycznej. Aby to zrobić, podajesz:
 - 1) imię i nazwisko tej osoby,

- 2) jej PESEL,
 - 3) numer dokumentu tożsamości,
 - 4) adres.
2. Wypłata odbywa się w kasie naszej placówki. Osoba, którą wskazałeś, odbierze gotówkę w określonej przez Ciebie kwocie i w ustalonym czasie. Musi okazać ważny dokument tożsamości.
 3. Każde zlecenie autowypłaty musisz zatwierdzić za pomocą swoich danych do autoryzacji, zgodnie z liczbą wymaganych podpisów.
 4. Osoba odbierająca pieniądze musi pokazać ten sam dokument tożsamości, którego dane podałeś w zleceniu.
 5. Szczegółowy opis działania usługi znajdziesz w przewodniku dla klienta.

C. Korzystanie z elektronicznych kanałów dostępu

§ 13

1. Z elektronicznych kanałów dostępu możesz korzystać 7 dni w tygodniu, 24 godziny na dobę, z wyjątkiem ograniczeń z § 14.
2. Przez elektroniczne kanały dostępu uzyskujesz dostęp do wszystkich rachunków: zarówno otwartych przed dniem aktywowania usługi, jak i po nim. Możesz jednak zawnieść o ograniczony dostęp do rachunków w elektronicznych kanałach dostępu.

D. Kiedy nie można korzystać z bankowości elektronicznej?

§ 14

1. Zablokujemy Ci dostęp do serwisu internetowego i uniemożliwimy wykonanie transakcji, jeśli:
 - 1) złożysz dyspozycję zablokowania dostępu do serwisu internetowego,
 - 2) trzy razy wpiszesz nieprawidłowy PIN do aplikacji mobilnej lub nieprawidłowe hasło stałe.
2. Możemy ograniczyć lub zablokować dostęp do serwisu internetowego lub czasowo zablokować wykonanie dyspozycji, jeśli:
 - 1) istnieją uzasadnione przyczyny, które wiążą się z bezpieczeństwem dostępu do serwisu internetowego i indywidualnych danych uwierzytelniających; również gdy podejrzewamy, że ktoś popełnił przestępstwo na Twoją szkodę,
 - 2) umyślnie doprowadziłeś(-aś) do nieautoryzowanej transakcji płatniczej lub mamy uzasadnione podejrzenie, że będziesz posługiwać się dostępem niezgodnie z regulaminem,
 - 3) korzystasz z serwisu internetowego niezgodnie z zasadami bezpieczeństwa określonymi w tym załączniku lub zagrażasz bezpieczeństwu korzystania z serwisu internetowego,
 - 4) konserwujemy serwis internetowy lub inne systemy teleinformatyczne związane z wykonywaniem umowy – poinformujemy Cię o tym z wyprzedzeniem na naszej stronie internetowej lub w bankowości internetowej, w tym mobilnej,
 - 5) usuwamy awarie, usterki lub nieprawidłowości działania w serwisie internetowym lub innych systemach teleinformatycznych związanych z wykonywaniem umowy,
 - 6) wymieniamy stosowane indywidualne dane uwierzytelniające – poinformujemy Cię o tym pisemnie lub na naszej stronie internetowej,
 - 7) mamy uzasadnione podejrzenie, że transakcje na Twoim rachunku mają związek z przestępstwem związanym z praniem pieniędzy lub finansowaniem terroryzmu,
 - 8) gdy na Twoim rachunku są zamrożone wartości majątkowe lub gdy wobec Ciebie należy stosować sankcje międzynarodowe albo embarga,
 - 9) nie możemy zastosować środków bezpieczeństwa finansowego; do tych sytuacji zaliczamy brak aktualnego dokumentu tożsamości Twojego lub osób upoważnionych do działania w Twoim imieniu.
3. Możemy uchylić ograniczenie albo blokadę dostępu do serwisu internetowego w przypadku z ust. 2 pkt 1, jeśli odpowiedni wniosek złożysz Ty lub Twój pełnomocnik. W takim przypadku albo wydajemy Ci nowe indywidualne dane uwierzytelniające, albo uchylamy ograniczenia lub blokady i zachowujesz dotychczasowe dane uwierzytelniające.
4. W przypadku z ust. 2 pkt 1 uchylenie:

- 1) ograniczenia lub blokady dostępu do serwisu internetowego następuje na podstawie Twojej dyspozycji telefonicznej lub złożonej w naszej dowolnej placówce,
 - 2) czasowej blokady dyspozycji następuje po tym, jak nasz pracownik skontaktuje się z Tobą telefonicznie lub pisemnie, a Ty potwierdzisz złożoną dyspozycję.
5. Z wyjątkiem ust. 6, informujemy Cię, że zamierzamy zablokować indywidualne dane uwierzytelniające w przypadkach z ust. 2 pkt 1 i 3, zanim je zablokujemy, a jeżeli nie jest to możliwe – telefonicznie, niezwłocznie po zablokowaniu.
6. Nie informujemy o zablokowaniu, jeżeli byłoby to nieuzasadnione ze względów bezpieczeństwa lub zabronione zgodnie z odrębnymi przepisami.
7. W przypadkach z ust. 2 pkt 4 i 5, ograniczenie lub blokada dostępu do serwisu internetowego lub czasowa blokada dyspozycji trwa możliwie krótko, tyle ile trwa usunięcie przyczyny.

E. Blokowanie i zastrzeganie dostępu

§ 15

1. Dostęp do serwisu internetowego oraz możliwość posługiwania się indywidualnymi danymi uwierzytelniającymi może zostać zablokowana przez:
 - 1) nas,
 - 2) Ciebie,
 - 3) przedstawiciela ustawowego małoletniego.
2. Możesz złożyć wniosek o zablokowanie dostępu do serwisu internetowego i uniemożliwić jednocześnie wykonanie transakcji.

§ 16

1. Jeśli jesteś użytkownikiem serwisu internetowego lub przedstawicielem ustawowym małoletniego, niezwłocznie zastrzeż dostęp do serwisu internetowego. Zrób to, jeżeli indywidualne dane uwierzytelniające zostały utracone, skradzione lub przywłaszczone albo ktoś użył ich bez uprawnień.
2. Zastrzeżenie z ust. 1 możesz wykonywać:
 - 1) w naszej placówce,
 - 2) przez call center lub pod innymi numerami telefonów, które wskazujemy i aktualizujemy w komunikacie w naszych placówkach lub na naszej stronie internetowej,
 - 3) w bankowości internetowej, w tym aplikacji mobilnej.
3. Możemy zmieniać numery telefonów służące do zastrzegania i blokowania dostępu do serwisu internetowego. Powiadomimy Cię o tym na naszej stronie internetowej oraz elektronicznie komunikatem w bankowości internetowej, w tym aplikacji mobilnej.
4. Nie możesz odwołać zastrzeżenia z ust. 1. Powoduje ono, że nie masz dalszego dostępu do serwisu internetowego.
5. Jeśli jesteś posiadaczem rachunku lub działającym w jego imieniu przedstawicielem ustawowym, możesz wystąpić z wnioskiem o nowe indywidualne dane uwierzytelniające, jeśli je wcześniej utracisz oraz zastrzeżesz. Możesz zachować ten sam identyfikator (login), pod warunkiem, że wydamy Ci nowe hasło dostępu.
6. Jeśli ktoś ukradnie lub przywłaszczy Twój telefon komórkowy albo stwierdzisz, że został on użyty w nieuprawniony sposób, zmień dane zgodnie z ust. 7. Dotyczy to telefonu oznaczonego jako telefon do autoryzacji lub zmiany numeru telefonu do autoryzacji.
7. Jeśli chcesz zmienić dane niezbędne do otrzymywania kodów SMS na nowe i:
 - 1) masz dotychczasowy numer telefonu do autoryzacji – możesz zmienić numer w serwisie internetowym, jeśli udostępniemy taką funkcjonalność; możemy skontaktować się z Tobą, aby zweryfikować zlecenie zmiany numeru tego telefonu i zmienić numer telefonu,
 - 2) nie masz dotychczasowego telefonu do autoryzacji, musisz złożyć odpowiednią dyspozycję w naszej placówce.

§ 17

1. Możemy zastrzec indywidualne dane uwierzytelniające, jeśli:
 - 1) umowa wygaśnie lub zostanie rozwiązana,

- 2) istnieją uzasadnione przyczyny związane z bezpieczeństwem indywidualnych danych uwierzytelniających, tzn. wiemy, że osoby trzecie weszły w ich posiadanie,
 - 3) podejrzewamy, że indywidualne dane uwierzytelniające zostały użyte w sposób nieuprawniony lub że umyślnie doprowadziłeś(-aś) do nieautoryzowanej transakcji płatniczej.
2. Z wyjątkiem ust. 3 informujemy Cię, że zamierzamy zastrzec indywidualne dane uwierzytelniające w przypadkach z ust. 1 pkt 2 i 3, zanim je zastrzeżemy, a jeżeli nie jest to możliwe – telefonicznie, niezwłocznie po zastrzeżeniu.
 3. Nie informujemy o zastrzeżeniu, jeżeli byłoby to nieuzasadnione ze względów bezpieczeństwa lub zabronione zgodnie z odrębnymi przepisami.

F. Udostępnianie danych o rachunku do usług płatniczych (PSD2)

§ 18

1. Jeśli korzystasz z serwisu internetowego i zgodzisz się na udostępnienie informacji o rachunku i transakcjach w nim, możemy udostępnić te informacje dostawcy, który świadczy usługi dostępu do informacji o rachunku.
2. Dostęp do informacji o rachunku z ust. 1 mogą mieć także dostawcy, którzy inicjują transakcje płatnicze dla użytkowników korzystających z serwisu internetowego.
3. Niezwłocznie potwierdzamy dostępność na rachunku kwoty niezbędnej do wykonania transakcji realizowanej kartą, jeżeli zawnioskuje o to dostawca wydający instrumenty płatnicze oparte na karcie płatniczej. Dostępność pieniędzy potwierdzamy, jeśli:
 - 1) Twój rachunek płatniczy jest dostępny online w momencie, w którym otrzymamy wniosek,
 - 2) zgodziłeś(-aś) się, abyśmy odpowiadali na tego rodzaju wnioski dostawcy wydającego instrumenty płatnicze oparte na karcie płatniczej,
 - 3) zgodnie z pkt 2 udzieliłeś(-aś), zanim wpłynął do nas pierwszy wniosek dotyczący potwierdzenia.
4. Dostawca wydający instrumenty płatnicze oparte na karcie płatniczej może wystąpić z wnioskiem z ust. 3, jeżeli:
 - 1) zgodziłeś(-aś) się, aby występował z wnioskiem z ust. 3,
 - 2) zainicjowałeś(-aś) transakcję płatniczą realizowaną kartą płatniczą przy użyciu opartego na tej karcie instrumentu płatniczego, który wydał dany dostawca,
 - 3) dostawca uwierzytni siebie wobec nas, zanim złoży wniosek z ust. 3, oraz porozumiewa się z nami w sposób bezpieczny.
5. Potwierdzenie z ust. 3 polega na tym, że udzielasz tylko odpowiedzi „tak” albo „nie” i nie podajesz salda rachunku. Odpowiedzi nie przechowujemy i wykorzystujemy ją tylko do wykonania transakcji realizowanej kartą płatniczą.
6. Potwierdzenie z ust. 3 nie umożliwia nam blokady pieniędzy na Twoim rachunku płatniczym.
7. Możesz zwrócić się do nas o przekazanie danych identyfikujących dostawcę z ust. 4 oraz udzielonej odpowiedzi z ust. 5.
8. Możemy odmówić dostępu do rachunku dostawcy świadczącemu usługę dostępu do informacji o rachunku lub dostawcy świadczącemu usługę inicjowania transakcji płatniczej. Mamy do tego prawo z przyczyn, które są obiektywnie uzasadnione i należycie udokumentowane lub mają związek z nielegalnym dostępem do rachunku takiego dostawcy, w tym z nieuprawnionym zainicjowaniem transakcji płatniczej. W takim przypadku w uzgodniony sposób informujemy Cię o odmowie dostępu do rachunku i jej przyczynach. Informujemy Cię, o ile jest to możliwe, zanim odmówimy dostępu, a jeżeli nie jest to możliwe – bezzwłocznie po takiej odmowie, najpóźniej w dniu roboczym następującym po dniu takiej odmowy. Nie informujemy o odmowie, jeżeli byłoby to nieuzasadnione ze względów bezpieczeństwa lub sprzeczne z odrębnymi przepisami. Dostawcy świadczącemu usługę dostępu do informacji o rachunku oraz dostawcy świadczącemu usługę inicjowania transakcji płatniczej umożliwiamy dostęp do rachunku niezwłocznie po tym, gdy ustanie przyczyna odmowy.

G. Aplikacja mobilna Nasz Bank oraz Nasz Bank Junior

G.1. Korzystanie z aplikacji

§ 19

1. Możesz pobrać aplikację Nasz Bank w Google Play na telefon z Androidem lub w App Store na telefon z iOS.
2. Po zainstalowaniu i uruchomieniu aplikacji ustawiasz PIN i wybierasz sposób logowania do aplikacji.
3. Do logowania możesz używać PIN-u lub danych biometrycznych, np. odcisku palca lub twarzy.
4. Aby korzystać z logowania biometrycznego, włącz tę funkcję na swoim zaufanym urządzeniu mobilnym i zarejestruj swoje cechy biometryczne. Musisz też włączyć tę funkcję w aplikacji. Aplikacja ani bank nie przetwarzamy Twoich danych biometrycznych.
5. Z aplikacji możesz korzystać tylko na zaufanym urządzeniu mobilnym.
6. Po aktywacji aplikacji możesz zatwierdzać transakcje złożone w serwisie internetowym przez:
 - 1) podanie kodu SMS lub
 - 2) zatwierdzenie powiadomienia push w aplikacji (autoryzacja mobilna). Jeśli masz więcej urządzeń z aktywną autoryzacją, powiadomienia przyjdą na wszystkie urządzenia.
7. Aby włączyć autoryzację mobilną, wpisz kod SMS otrzymany od banku.
8. Jeśli chcesz wrócić do autoryzacji SMS, możesz:
 - 1) poprosić o zmianę osobiście w oddziale banku,
 - 2) zrobić to samodzielnie w Internet Bankingu w ustawieniach lub podczas wykonywania przelewu,
 - 3) usunąć profil w aplikacji. Jeśli usuniesz aplikację z urządzenia mobilnego bez wcześniejszego usunięcia profilu w aplikacji – nie przywróci to autoryzacji SMS.
9. Jeśli trzy razy wpiszesz błędny PIN w aplikacji lub ją odinstalujesz, autoryzacja mobilna nie zmieni się automatycznie na hasła SMS.
10. Po aktywacji aplikacji, dla Twojego bezpieczeństwa, niektórych funkcji możesz używać dopiero po pewnym czasie. Na przykład, nie zmienisz limitów w ciągu 24 godzin ani nie skorzystasz z BLIKa w ciągu 1 godziny.
11. Przelewy, BLIK i smartKARTĘ możesz używać tylko na urządzeniu z włączoną autoryzacją mobilną.
12. Jeśli dezaktywujesz aplikację na swoim telefonie, zgoda na korzystanie z bankowości mobilnej na tym urządzeniu zostaje cofnięta. Jeśli usuniesz aplikację bez jej dezaktywacji, zgoda nadal obowiązuje.
13. Jeśli logowanie danymi biometrycznymi się nie uda, zaloguj się PIN-em.
14. Jeśli wpiszesz trzy razy błędny PIN, aplikacja automatycznie zablokuje dostęp do bankowości.
15. Licznik błędnych prób zeruje się po poprawnym zalogowaniu, o ile aplikacja nie została zablokowana.
16. Aby odblokować aplikację:
 - 1) odinstaluj i zainstaluj ją ponownie na zaufanym telefonie – jeśli posiadasz autoryzację na hasła SMS,
 - 2) zgłoś się do naszej placówki – jeśli posiadasz autoryzację mobilną.
17. Dziecko może używać Nasz Bank Junior tylko za zgodą opiekuna (rodzica). Aktywacja odbywa się w aplikacji dziecka i w aplikacji rodzica.
18. Rodzic na bieżąco sprawdza, czy dziecko poprawnie wykonuje transakcje.
19. Rodzic lub opiekun wyjaśnia dziecku, jak używać aplikacji i jak dbać o bezpieczeństwo danych.
20. Wszystkie szczegóły działania aplikacji znajdziesz w przewodnikach po Nasz Bank i Nasz Bank Junior.

G.2. Zasady bezpieczeństwa

§ 20

1. Jako użytkownik musisz:
 - 1) chronić swój identyfikator, hasło do bankowości internetowej, kod SMS, PIN do aplikacji i urządzenie mobilne, aby nikt nieuprawniony ich nie używał,
 - 2) niezwłocznie zgłosić utratę, kradzież, przywłaszczenie lub nieuprawnione użycie telefonu z aplikacją,
 - 3) niezwłocznie zgłosić, jeśli ktoś używa aplikacji, BLIKa lub smartKARTY bez Twojej zgody,
 - 4) niezwłocznie zgłosić, jeśli ktoś nieuprawniony uzyska dostęp do Twojego konta przez BLIK,

- 5) nie udostępniać aplikacji ani kodu BLIK osobom nieuprawnionym,
 - 6) chronić swoje dane do logowania oraz nie udostępniać ich nikomu,
 - 7) używać kodu BLIK tylko zgodnie z jego przeznaczeniem,
 - 8) przechowywać PIN do aplikacji i urządzenia z aplikacją w bezpieczny sposób.
2. Jeśli utracisz telefon z aplikacją, zgłoś to:
 - 1) osobiście w naszej placówce,
 - 2) telefonicznie dzwoniąc do naszej dowolnej placówki w godzinach jej pracy,
 - 3) telefonicznie na call center.
 3. Po takim zgłoszeniu zablokujemy BLIKa, smartKARTĘ lub dostęp do aplikacji.
 4. Zablokowanie jest bezterminowe. Nie możesz wtedy korzystać z tych usług ani aplikacji.
 5. Po zablokowaniu BLIKa lub smartKARTY możesz ponownie je włączyć w aplikacji, o ile aplikacja nie została zablokowana.
 6. Możesz samodzielnie w każdej chwili włączyć lub wyłączyć BLIKa lub smartKARTĘ w ustawieniach aplikacji.
 7. Jeśli udostępnisz telefon, aplikację lub PIN osobom trzecim, ponosisz za to odpowiedzialność.
 8. Korzystaj tylko z aplikacji pobranej z wiarygodnego źródła, czyli ze sklepów Google Play lub App Store.
 9. Zalecamy, żebyś chronił swój telefon przez:
 - 1) ustawienie blokady ekranu,
 - 2) zainstalowanie programu antywirusowego.
 10. Nie otwieraj na telefonie e-maili, załączników ani linków z nieznanych źródeł lub od nieznanych osób.
 11. Podczas korzystania z aplikacji komunikacja między telefonem a bankiem jest szyfrowana i bezpieczna.
 12. Nie instaluj na telefonie nielegalnych lub podejrzanych programów, które otrzymujesz e-mailem lub pobierasz z internetu.
 13. Nigdy nie prosimy Cię o ujawnienie haseł ani instalowanie dodatkowych programów lub certyfikatów.
 14. Nie używaj aplikacji na telefonie, jeśli usunąłeś w nim fabryczne ograniczenia systemowe.

G.3. Ograniczenia i limity w aplikacji mobilnej

§ 21

1. Możemy czasowo zablokować Ci usługę BLIK, smartKARTĘ lub aplikację mobilną w przypadku:
 - 1) uzasadnionych przyczyn związanych z bezpieczeństwem usługi,
 - 2) stwierdzenia dokonania lub próby dokonania transakcji przez osobę nieuprawnioną,
 - 3) użytkownika usługi w sposób niezgodny z prawem,
 - 4) umyślnego doprowadzenia do nieautoryzowanych transakcji.
2. Zablokujemy Ci dostęp do aplikacji, jeśli:
 - 1) złożysz dyspozycję zablokowania lub dezaktywacji aplikacji;
 - 2) 3-krotnie wprowadzisz nieprawidłowy PIN do aplikacji.
3. Możemy częściowo ograniczyć lub zablokować Ci dostęp do aplikacji lub czasowo zablokować wykonanie operacji w następujących przypadkach:
 - 1) z uzasadnionych przyczyn związanych z bezpieczeństwem, czyli gdy:
 - a) dowiemy się lub będziemy podejrzewać, że dyspozycje w aplikacji składają osoby nieuprawnione,
 - b) istnieje zagrożenie przechwycenia Twoich danych dostępowych przez złośliwe oprogramowanie,
 - c) Twoje dane dostępowe są używane przez automatyczne programy logujące się z dużą częstotliwością,
 - d) wykorzystujesz system lub rachunki w sposób niezgodny z prawem,
 - e) wykonujesz działania zagrażające bezpieczeństwu systemu i danych w nim przetwarzanych;

- 2) podejrzewamy nieuprawnione użycie aplikacji, zaufanego urządzenia mobilnego, indywidualnych danych uwierzytelniających lub umyślne doprowadzenie do nieautoryzowanej dyspozycji;
- 3) dowiemy się o zagrożeniu bezpieczeństwa operacji;
- 4) będziemy przeprowadzać konserwację aplikacji lub innych systemów związanych z jej działaniem, o czym poinformujemy Cię o tym wcześniej w aplikacji mobilnej;
- 5) gdy wykonujemy czynności mające na celu usunięcie awarii, usterek lub nieprawidłowości działania aplikacji lub innych systemów związanych z jej obsługą.
4. Uchylimy ograniczenie albo blokadę dostępu do aplikacji w przypadkach z ust. 3 pkt 1-3, jeżeliawnioskujesz o nowe indywidualne dane uwierzytelniające.
5. W przypadkach z ust. 3 pkt 2-5, ograniczenie lub blokada dostępu do aplikacji lub czasowa blokada dyspozycji będzie trwała tylko tak długo, jak to konieczne, aby usunąć przyczynę ograniczenia lub blokady.
6. Zablokujemy dostęp do aplikacji, jeśli wygasną umowy, które z nami zawarłeś.

§ 22

1. Ze względów bezpieczeństwa ustalamy limity dla transakcji BLIK i smartKARTY.
2. Dienne limity dla transakcji BLIK przedstawia poniższa tabela.

Rodzaj limitu BLIK	wartość standardowa	wartość maksymalna	limit ilościowy
Dzienny limit wypłat gotówki	500 PLN	5 000 PLN	10 szt.
Dzienny limit transakcji bezgotówkowych w tym transakcji internetowych oraz BLIK Płacę Później – tylko pow. 18 r.ż.	do 18 r.ż.: 500 PLN pow. 18 r.ż.: 1 000 PLN	5 000 PLN 5 000 PLN	100 szt. 100 szt.
Limit pojedynczej transakcji przelew na telefon BLIK, prośby o przelew BLIK	1 000 PLN	1 000 PLN	
Dzienny limit wszystkich transakcji przelewów na telefon BLIK, prośby o przelew BLIK	5 000 PLN	5 000 PLN	
Dzienny limit globalny BLIK (suma wypłat gotówki, transakcji bezgotówkowych, internetowych, prośby o przelew BLIK oraz BLIK Płacę Później)	5 000 PLN	5 000 PLN	

3. W usłudze smartKARTA obowiązują następujące limity:
 - 1) dziennie możesz wypłacić do 1 500 PLN,
 - 2) jednorazowo możesz wpłacić do 5 000 PLN,
 - 3) dziennie możesz wpłacić do 20 000 PLN,
 - 4) w miesiącu możesz wpłacić do 50 000 PLN.
4. Możesz prosić o indywidualne limity, oprócz limitów globalnych i ilościowych.
5. My decydujemy o ostatecznej wysokości limitów.
6. Przy wpłatach we wpłatomatach możemy zapytać Cię o pochodzenie środków.

G.4. BLIK w aplikacji mobilnej Nasz Bank

§ 23

1. Usługa BLIK pozwala na dokonywanie transakcji BLIK przez aplikację mobilną.
2. Udostępniamy Ci BLIK bez dodatkowego wniosku. Aby uruchomić BLIKa, włącz go w ustawieniach aplikacji.
3. Z BLIKa może korzystać tylko osoba, która ma aplikację na zaufanym urządzeniu.
4. Aby używać BLIK, musisz jednocześnie:
 - 1) mieć zaufane urządzenie,
 - 2) mieć konto w złotych (PLN), z którego będą realizowane transakcje BLIK,

- 3) mieć zainstalowaną aplikację na telefonie,
 - 4) włączyć usługę BLIK w ustawieniach aplikacji,
 - 5) zaakceptować zasady korzystania z usługi.
5. Musisz korzystać z BLIK zgodnie z prawem, regulaminem i przewodnikiem po aplikacji.
6. Poniżej wyjaśniamy pojęcia związane z BLIKiem:
- 1) baza powiązań BLIK – lista odbiorców przelewów na telefon BLIK prowadzona przez Polski Standard Płatności (PSP),
 - 2) BLIK/usługa BLIK – usługa, którą udostępniamy Ci w naszej aplikacji mobilnej; dzięki niej możesz wykonywać płatności na zasadach opisanych w tym załączniku,
 - 3) BLIK Płać Później – usługa oferowana przez zewnętrznego dostawcę (PSP), która pozwala Ci zapłacić za zakupy w sklepach internetowych do 30 dni później, w ramach przyznanego limitu. Usługa jest dostępna w naszej aplikacji mobilnej po zawarciu przez Ciebie umowy z PSP. Szczegółowe zasady znajdziesz w „Regulaminie zawierania Umowy kredytowej BLIK Płać Później”. Z usługi mogą korzystać wyłącznie osoby pełnoletnie.
 - 4) kod BLIK – 6-cyfrowy kod potrzebny do transakcji BLIK, generowany w aplikacji,
 - 5) płatności powtarzalne BLIK – funkcja w aplikacji mobilnej, która pozwala Ci automatycznie opłacać cykliczne płatności (np. abonamenty) za pomocą BLIKA. Aby ją włączyć, wybierasz płatność powtarzalną BLIK na stronie sprzedawcy, wpisujesz kod BLIK wygenerowany w aplikacji, a następnie autoryzujesz pierwszą płatność i wyrażasz zgodę na jej powtarzanie na warunkach sprzedawcy wyświetlonych w aplikacji; po tym kolejne płatności będą realizowane automatycznie;
 - 6) płatność BLIK – płatność za produkty lub usługi w sklepie, punkcie usługowym lub internecie przy użyciu kodu BLIK; jest to przelew zewnętrzny lub wewnętrzny,
 - 7) płatności powtarzalne BLIK – to funkcjonalność aplikacji umożliwiająca automatyczne realizowanie cyklicznych transakcji za pomocą systemu BLIK, na rzecz podmiotu oferującego tę metodę płatności; wybierasz płatność powtarzalną BLIK na stronie sprzedawcy, wpisujesz kod BLIK z aplikacji, a następnie autoryzujesz pierwszą płatność powtarzalną i wyrażasz zgodę na jej powtarzanie na warunkach sprzedawcy zaprezentowanych na ekranie aplikacji; o udostępnieniu usługi powiadomimy Cię na naszej stronie internetowej;
 - 8) podział rachunku BLIK – usługa umożliwiająca podział kwoty płatności na kilka osób i rozliczenie jej między nimi za pomocą aplikacji mobilnej;
 - 9) prośba o przelew BLIK – przelew krajowy, który zaczyna się od wysłania prośby o płatność. Prośbę może wysłać tylko użytkownik z aktywną usługą BLIK. Przelew realizujemy wyłącznie z rachunku powiązanego z usługą BLIK. Trafia on na rachunek osoby wysyłającej prośbę, przypisany do numeru telefonu wskazanego w prośbie. W tym rodzaju przelewu numer telefonu jest jedynym identyfikatorem osoby wysyłającej prośbę.
 - 10) przelew na telefon BLIK – przelew natychmiastowy w kraju wyrażony w złotych (PLN), wykonany w aplikacji mobilnej na numer telefonu odbiorcy zarejestrowanego w bazie powiązań BLIK,
 - 11) PSP – Polski Standard Płatności sp. z o.o. w Warszawie, który zarządza systemem BLIK,
 - 12) rachunek BLIK – rachunek prowadzony przez nas, który wybierasz w aplikacji, z którego realizujesz płatności oraz inne transakcje BLIK,
 - 13) system rozliczeń BLIK – system międzybankowy, w którym rozliczamy transakcje BLIK; informacje o bankach uczestniczących w systemie znajdziesz na stronie internetowej PSP, która zarządza tym systemem,
 - 14) szybka płatność BLIK – funkcja w naszej aplikacji, dzięki której możesz wygenerować kod BLIK bez logowania się do aplikacji,
 - 15) transakcje BLIK – gotówkowe lub bezgotówkowe (krajowe transakcje płatnicze), których skutkiem jest obciążenie rachunku BLIK z tytułu:
 - a) zapłaty za towary lub usługi nabyte w serwisie internetowym lub aplikacji podmiotu oferującego te towary lub usługi,
 - b) wypłaty gotówki w wybranych bankomatach oraz terminalach płatniczych,

- c) płatności za towary i usługi w oznaczonych punktach wyposażonych w terminale płatnicze lub inne urządzenia umożliwiające wykonanie operacji zlecanych przez kanał mobilny,
- 16) transakcje zbliżeniowe BLIK – usługa, która pozwala Ci płacić telefonem zbliżeniowo w terminalach, bez wpisywania kodu BLIK. Korzystamy przy tym z zabezpieczeń Twojego urządzenia mobilnego oraz naszych metod potwierdzania płatności. Możemy wprowadzić limity kwotowe dla takich transakcji oraz uzależnić sposób ich potwierdzenia od kwoty lub poziomu ryzyka; o udostępnieniu usługi powiadomimy Cię na naszej stronie internetowej;
- 17) wypłata BLIK – transakcja, w której wypłacasz gotówkę w bankomacie lub terminalu w sklepie bez użycia karty płatniczej.

§ 24

1. W ramach BLIK możesz wykonywać następujące transakcje:
 - 1) wypłacać gotówkę w bankomatach z oznaczeniem BLIK,
 - 2) wypłacać gotówkę w punktach handlowo-usługowych w ramach usługi cash back, jeśli punkt akceptuje BLIK,
 - 3) płacić za towary i usługi w złotych:
 - a) w terminalach POS u sprzedawców oznaczonych znakiem BLIK,
 - b) w internecie u sprzedawców oznaczonych znakiem BLIK,
 - 4) wysyłać przelewy na telefon BLIK,
 - 5) odbierać przelewy na telefon BLIK,
 - 6) wysyłać prośby o przelew BLIK,
 - 7) korzystać z płatności powtarzalnych BLIK, o ile udostępniliśmy taką usługę,
 - 8) korzystać z usługi BLIK Płacę Później.
2. Możesz wykonywać transakcje BLIK tylko do wysokości dostępnego salda i w ramach ustalonych limitów dla BLIKa.
3. Zasady naszej odpowiedzialności za transakcje BLIK są takie same, jak zasady odpowiedzialności za płatności wykonywane innymi instrumentami płatniczymi.

G.5. Transakcje w usłudze BLIK

§ 25

1. Transakcje BLIK:
 - 1) możesz wykonywać tylko w złotych,
 - 2) możesz wykonywać tylko na terytorium Polski,
 - 3) rozliczają się na Twoim koncie w złotych.
2. Aby wykonać transakcję BLIK, musisz ją autoryzować zgodnie z punktami opisanymi poniżej.
3. Uznajemy, że zlecenie BLIK dotarło w momencie, gdy zatwierdzisz je w aplikacji.
4. Autoryzacja transakcji BLIK w terminalu POS, w bankomacie lub w internecie wygląda tak:
 - 1) uruchamiasz aplikację za pomocą PIN-u lub logowania biometrycznego,
 - 2) generujesz kod BLIK w aplikacji,
 - 3) wpisujesz kod BLIK w terminalu POS, w bankomacie lub na stronie internetowej,
 - 4) potwierdzasz transakcję w aplikacji.
5. Przelew na telefon BLIK trafia na rachunek przypisany do numeru telefonu w bazie powiązań BLIK. Numer telefonu podajesz w aplikacji lub systemie bankowym. Aby otrzymywać przelewy na telefon BLIK, musisz zarejestrować swój numer telefonu i numer rachunku w bazie powiązań BLIK. Od momentu rejestracji każdy przelew wysłany na ten numer telefonu trafi na wskazany rachunek. Jeśli zmienisz numer telefonu, zaktualizuj dane w bazie powiązań BLIK, aby nadal otrzymywać przelewy. Zrobisz to w aplikacji lub w naszej placówce. Możesz powiązać tylko jeden numer telefonu z jednym numerem rachunku.
6. Prawidłowa dyspozycja przelewu na telefon BLIK powinna zawierać:
 - 1) numer telefonu odbiorcy,
 - 2) kwotę w złotych, nie większą niż limit i nie większą niż saldo na Twoim koncie,
 - 3) dane identyfikujące odbiorcę,
 - 4) tytuł przelewu.

7. Dyspozycja przelewu na prośbę BLIK, może być wykonana po otrzymaniu w aplikacji prośby od innego użytkownika BLIK lub klienta innego banku. Ty jesteś płatnikiem, a osoba wysyłająca prośbę – nadawcą.
8. Prawidłowa prośba o przelew BLIK, powinna zawierać:
 - 1) kwotę w złotych,
 - 2) tytuł przelewu,
 - 3) imię, nazwisko i numer telefonu płatnika zapisane w Twoim telefonie. Bank pokaże Ci dodatkowo imię i nazwisko nadawcy, a czasem jego numer rachunku BLIK lub inny rachunek nadawcy powiązany z systemem BLIK.
9. Nadawca może anulować prośbę w aplikacji przed zatwierdzeniem przelewu przez płatnika. Prośba jest ważna 72 godziny od wysłania.
10. Pozwalamy wysyłać więcej niż jedną prośbę o przelew BLIK, ale dla bezpieczeństwa liczba próśb wysyłanych jednocześnie może być jednak ograniczona.
11. Możesz całkowicie wyłączyć odbieranie próśb o przelew BLIK lub zablokować prośby od wybranego użytkownika i numeru telefonu. Blokadę możesz odwołać.
12. Po otrzymaniu prośby o przelew BLIK możesz ją odrzucić lub wykonać przelew. Zlecenie przelewu na prośbę BLIK realizowane jest na numer telefonu wskazany w prośbie, na kwotę i tytuł podane przez nadawcę.
13. Korzystanie z BLIKa wymaga:
 - 1) wybrania rachunku, z którego będą pobierane lub na który będą wpływać środki z transakcji BLIK,
 - 2) zarejestrowania numeru telefonu w bazie powiązań BLIK, aby inni klienci mogli wysyłać przelewy na telefon,
 - 3) posiadania aktywnej usługi BLIK i zarejestrowanego numeru telefonu, jeśli chcesz korzystać z próśb o przelew BLIK.
14. Możesz zmieniać powyższe ustawienia w aplikacji. Zmiana wymaga potwierdzenia PIN-em.
15. Realizujemy transakcje BLIK:
 - 1) przez całą dobę,
 - 2) w dniu ich otrzymania.
16. Nie przyjmujemy transakcji BLIK, jeśli:
 - 1) konto powiązane z BLIK jest zamknięte,
 - 2) podałeś nieprawidłowe dane przy autoryzacji,
 - 3) przekroczyłeś czas zatwierdzenia transakcji w aplikacji,
 - 4) kod BLIK stracił ważność,
 - 5) kwota transakcji przekracza limit BLIK,
 - 6) kwota transakcji przekracza dostępne saldo.
17. Akceptant może odmówić przyjęcia transakcji BLIK, jeśli:
 - 1) podałeś błędne dane przy autoryzacji,
 - 2) nie można uzyskać zgody banku na realizację transakcji.
18. Anulowanie transakcji BLIK jest możliwe do momentu zatwierdzenia jej w aplikacji. Po zatwierdzeniu możesz anulować transakcję tylko u akceptanta, jeśli on daje taką możliwość.

§ 26

1. Kod BLIK używany do autoryzacji:
 - 1) jest jednorazowy i działa maksymalnie 120 sekund od momentu wygenerowania; aplikacja pokaże Ci, kiedy zbliża się koniec ważności kodu,
 - 2) przestaje działać po upływie czasu ważności lub po użyciu do autoryzacji transakcji, dla której został wygenerowany,
 - 3) w danym momencie dla jednego użytkownika może istnieć tylko jeden ważny kod BLIK.
2. Przelewy na telefon BLIK, prośby o przelew BLIK wychodzące z banku są realizowane jako:
 - 1) przelewy wewnętrzne – jeśli odbiorca ma konto w naszym banku,
 - 2) przelewy Express Elixir – jeśli odbiorca ma konto w innym banku.
3. Aby zlecić przelew w aplikacji, musisz autoryzować dyspozycję swoimi danymi:

- 1) PIN-em do aplikacji lub
- 2) danymi biometrycznymi,
- 3) a jeśli dyspozycję składa dziecko, także zgodą rodzica lub opiekuna.
4. Autoryzacja transakcji BLIK oznacza, że zgadzasz się na jej wykonanie. Po zatwierdzeniu nie można cofnąć zgody.

G.6. BLIK w aplikacji Nasz Bank Junior

§ 27

1. Rodzic może udostępnić dziecku kod BLIK, jeśli włączy odpowiednie ustawienia w swojej aplikacji Nasz Bank. Transakcja BLIK wygląda tak:
 - 1) dziecko w aplikacji Nasz Bank Junior prosi o kod BLIK,
 - 2) rodzic potwierdza prośbę w swojej aplikacji,
 - 3) kod BLIK pojawia się w aplikacji Nasz Bank Junior i dziecko używa go przy płatności,
 - 4) rodzic potwierdza płatność wykonaną przez dziecko przy użyciu kodu BLIK.
2. Dienne limity transakcji BLIK są następujące:

Rodzaj limitu BLIK	wartość standardowa	wartość maksymalna	limit ilościowy
wypłaty gotówki	500 PLN	500 PLN	10 szt.
transakcje bezgotówkowe, w tym	500 PLN	500 PLN	100 szt.
transakcje internetowe	500 PLN	500 PLN	100 szt.
dzienny limit globalny BLIK	500 PLN	500 PLN	

G.7. Usługa smartKARTA

§ 28

1. Usługa smartKARTA pozwala Ci wykonać transakcję w bankomacie lub wpłatomacie naszego Banku za pomocą kodu QR wygenerowanego w aplikacji mobilnej Nasz Bank. Dzięki temu nie musisz dotykać bankomatu.
2. Udostępniamy Ci usługę smartKARTA bez składania dodatkowego wniosku. Włączasz ją samodzielnie w ustawieniach aplikacji mobilnej.
3. Z usługi smartKARTA możesz korzystać tylko wtedy, gdy masz zainstalowaną aplikację mobilną Nasz Bank na zaufanym urządzeniu.
4. Aby korzystać z usługi smartKARTA, musisz spełnić wszystkie poniższe warunki:
 - 1) musisz mieć zaufane urządzenie mobilne,
 - 2) musisz mieć rachunek w złotych (PLN), z którego będą realizowane transakcje,
 - 3) musisz mieć zainstalowaną aplikację mobilną Nasz Bank na swoim urządzeniu.
5. Korzystając z usługi smartKARTA, musisz działać zgodnie z przepisami prawa, w tym regulaminem oraz przewodnikiem po aplikacji mobilnej.

§ 29

1. W ramach usługi smartKARTA możesz wykonywać następujące transakcje:
 - 1) wypłacać gotówkę w naszych bankomatach,
 - 2) wpłacać gotówkę w naszych wpłatomatach.
 Listę naszych wpłatomatów i bankomatów znajdziesz na naszej stronie internetowej.
2. Możesz wykonywać transakcje w ramach usługi smartKARTA tylko do wysokości dostępnych środków na rachunku i w ramach limitów ustalonych dla tej usługi.

§ 30

1. Transakcje w usłudze smartKARTA:
 - 1) są wykonywane wyłącznie w polskich złotych,
 - 2) są rozliczane na rachunkach prowadzonych w polskich złotych.
2. Każda transakcja w usłudze smartKARTA wymaga autoryzacji na zasadach opisanych w ust. 4.

3. Za moment otrzymania przez nas zlecenia płatniczego uznajemy chwilę, w której autoryzujesz transakcję smartKARTA.
4. Autoryzacja transakcji w usłudze smartKARTA w naszych bankomatach lub wpłatomatach odbywa się w następujący sposób:
 - 1) uruchamiasz aplikację mobilną Nasz Bank, używając PIN-u do aplikacji lub danych biometrycznych,
 - 2) wybierasz w aplikacji odpowiednią operację (wpłata lub wypłata) oraz kwotę transakcji,
 - 3) skanujesz kod QR wyświetlony na ekranie bankomatu lub wpłatomatu,
 - 4) potwierdzasz transakcję w aplikacji mobilnej Nasz Bank.
5. Transakcje w usłudze smartKARTA realizujemy:
 - 1) przez całą dobę,
 - 2) w dniu ich otrzymania.
6. Odmówimy realizacji transakcji w usłudze smartKARTA, jeżeli:
 - 1) podczas autoryzacji podasz nieprawidłowe dane,
 - 2) nie potwierdzisz transakcji w czasie wskazanym w aplikacji mobilnej,
 - 3) kwota transakcji przekroczy limit obowiązujący w usłudze smartKARTA,
 - 4) kwota transakcji przekroczy dostępne środki na rachunku.
7. Możesz anulować transakcję smartKARTA do momentu jej autoryzacji. Po dokonaniu autoryzacji anulowanie transakcji nie jest możliwe.

G.8. Funkcjonalności dostępne w aplikacji dziecka – Nasz Bank Junior

§ 31

1. W aplikacji Nasz Bank Junior dziecko może m.in.:
 - 1) sprawdzać swoje konta,
 - 2) zakładać, przeglądać i zamykać skarbonki,
 - 3) robić przelewy (wewnętrzne i wychodzące) oraz odbierać przelewy,
 - 4) korzystać z BLIKA,
 - 5) podglądać kartę płatniczą,
 - 6) korzystać z mapy nagród (nagrody za aktywność i oszczędzanie).
2. Dodatkowo rodzic w aplikacji Nasz Bank może zarządzać aplikacją swojego dziecka:
 - 1) udostępniać kod BLIK i zatwierdzać transakcje,
 - 2) zmieniać limity BLIK,
 - 3) zmieniać limity karty płatniczej,
 - 4) blokować i zastrzegać kartę,
 - 5) doładować telefon na kartę,
 - 6) mieć pełny podgląd produktów dziecka.
3. Rodzic może w pełni kontrolować finanse dziecka – w swojej aplikacji ma dostęp do wszystkich jego produktów.
4. Pozostałe funkcje aplikacji znajdziesz w przewodniku po aplikacji Nasz Bank Junior.

G.9. Funkcjonalności dostępne w aplikacji Nasz Bank

§ 32

1. W aplikacji Nasz Bank możesz korzystać z następujących funkcjonalności:
 - 1) podgląd konta:
 - a) sprawdzisz saldo i historię operacji,
 - b) przejrzysz szczegóły rachunku,
 - c) sprawdzisz blokady środków, np. transakcje kartowe,
 - d) zmienisz limity transakcji;
 - 2) wykonywanie przelewów:
 - a) przelew własny – pomiędzy swoimi rachunkami,
 - b) przelew krajowy,
 - c) przelew do ZUS i US,
 - d) przelew europejski (SEPA – tylko w euro),
 - e) przelew QR,

- f) doładowujesz telefon;
- g) wymienisz walutę w kantorze,
- 3) lokaty:
 - a) sprawdzisz szczegóły lokaty,
 - b) założysz lokatę – tylko w Internet Bankingu, nie zrobisz tego w Internet Bankingu dla Firm,
 - c) zlikwidujesz lokatę – tylko w Internet Banking, jeśli założyłeś ją w bankowości internetowej, nie zrobisz tego w Internet Bankingu dla Firm;
- 4) kredyty:
 - a) sprawdzisz szczegóły kredytu,
 - b) wyświetlisz harmonogram spłaty;
- 5) karty płatnicze:
 - a) nadasz lub zmienisz PIN do karty,
 - b) aktywujesz, zablokujesz lub zastrzeżesz kartę,
 - c) zmienisz limity,
 - d) włączysz lub wyłączysz płatności zbliżeniowe,
 - e) zamówisz nową kartę – wyłącznie w Internet Bankingu;
- 6) dodatkowo możesz:
 - a) płacić BLIKiem – jeśli chcesz korzystać z BLIKa w internet Bankingu dla Firm – musisz o niego zawnioskować w naszej placówce,
 - b) przelewać BLIKiem na numer telefonu,
 - c) korzystać z usługi BLIK Płacę Później, która pozwala odroczyć płatność za zakupy internetowe do 30 dni w ramach przyznanego limitu,
 - d) korzystać z kodów QR,
 - e) potwierdzać transakcje w internecie (3D Secure),
 - f) sprawdzić powiadomienia i autoryzacje,
 - g) bezdotykowo wpłacić lub wypłacić gotówkę z bankomatu – przy użyciu smartKARTY,
 - h) skontaktować się z nami,
 - i) zweryfikować naszego pracownika podczas rozmowy telefonicznej z Tobą,
 - j) korzystać z aplikacji Nasz Bank Junior – aplikacji dla swojego dziecka;
- 7) w ustawieniach:
 - a) zmienisz PIN do aplikacji,
 - b) włączysz lub wyłączysz logowanie biometryczne,
 - c) zmienisz podstawowe ustawienia Twoich usług,
 - d) zablokujesz dostęp do aplikacji lub do wszystkich kanałów dostępu przez internet.
- 2. Pozostałe funkcje aplikacji znajdziesz w przewodnikach po aplikacji Nasz Bank.
- 3. Dodanie nowych usług lub rozszerzenie funkcji istniejących w aplikacji mobilnej (opisanych wyżej) nie jest zmianą regulaminu, pod warunkiem, że nie zwiększa Twoich kosztów ani nie narusza Twoich praw jako użytkownika. O każdej takiej zmianie będziemy Cię informować na naszej stronie internetowej lub w komunikatach w bankowości internetowej, w tym aplikacji mobilnej.
- 4. Możemy aktualizować, ulepszać lub zastępować aplikację nowymi wersjami. W wyjątkowych sytuacjach możemy wycofać starszą wersję – wtedy nie będzie można jej pobrać, aktywować ani się do niej zalogować. Poinformujemy Cię o tym z wyprzedzeniem. Przekażemy też, co trzeba zrobić, np. pobrać i zainstalować nową wersję aplikacji.
- 5. Możemy wysłać Ci w aplikacji mobilnej Nasz Bank powiadomienie push. Może to być zwykła informacja albo prośba o autoryzację.
- 6. Powiadomienie push może służyć m.in. do:
 - 1) poinformowania Cię o planowanym kontakcie naszego pracownika – wysyłamy wiadomość z imieniem i nazwiskiem pracownika, danymi placówki, datą rozmowy i celem kontaktu,
 - 2) poproszenia Cię o zgodę lub odmowę kontaktu – oprócz informacji z ppkt 1, możesz potwierdzić lub odrzucić kontakt,
 - 3) potwierdzenia tożsamości naszego pracownika – podczas rozmowy telefonicznej możesz sprawdzić, że kontaktuje się z Tobą prawdziwy pracownik Banku,

- 4) potwierdzenia Twojej tożsamości – w razie potrzeby weryfikujemy Twoje dane w aplikacji, żeby mieć pewność, że rozmawiamy z właściwym użytkownikiem.

H. Limity transakcji w bankowości internetowej, w tym mobilnej

§ 33

1. Standardowe limity pojedynczej transakcji oraz limity wszystkich transakcji w ciągu dnia w serwisie internetowym w Internet Banking (IB) oraz Internet Banking dla Firm (IBF) przedstawiają tabele:

- 1) limity transakcji do rachunku złotówkowego:

Kanał dostępu/rodzaj przelewu	Limit pojedynczej operacji	Limit wszystkich operacji w ciągu dnia
Serwis internetowy IB/IBF	5 000 PLN	20 000 PLN
Aplikacja mobilna Nasz Bank	1 000 PLN	3 000 PLN
Przelew BlueCash	3 000 PLN	15 000 PLN (max 3 szt. po 3 000 PLN)
Przelew Express ELIXIR	3 000 PLN	15 000 PLN (max 3 szt. po 3 000 PLN)
Łączny limit w bankowości internetowej, w tym mobilnej	5 000 PLN	20 000 PLN

- 2) limity transakcji do rachunku walutowego:

Kanał dostępu	Limit pojedynczej operacji	Limit wszystkich operacji w ciągu dnia
Serwis internetowy IB/IBF	2 000 EUR/USD/GBP	5 000 EUR/USD/GBP
Aplikacja mobilna	1 000 EUR/USD/GBP	2 000 EUR/USD/GBP

2. Limity dotyczą transakcji na rachunku.
3. Limity w aplikacji mobilnej wliczają się w limity serwisu internetowego i nie stanowią odrębnych limitów.
4. Limity przelewów ekspresowych wliczają się w limity aplikacji oraz w limity serwisu internetowego – nie są one traktowane jako osobny, dodatkowy limit.
5. Dla przelewów ekspresowych obowiązują również limity ilościowe, liczone łącznie dla dyspozycji składanych w placówce, w serwisie internetowym oraz w aplikacji mobilnej. Limit wynosi 5 przelewów dziennie dla każdego rodzaju osobno, tj.:
- 1) Express ELIXIR: do 5 przelewów po 30 000 PLN, łącznie 150 000 PLN,
 - 2) BlueCash: do 5 przelewów po 20 000 PLN, łącznie 100 000 PLN.
- Szczegóły znajdują się w załączniku nr 1 do Regulaminu: Przelewy natychmiastowe Express ELIXIR i BlueCash.
6. Jeśli przelewy w Internet Bankingu dla Firm autoryzowane są w aplikacji mobilnej, to można je zatwierdzać do wysokości limitu ustalonego dla IBF.
7. Możesz wnioskować o indywidualne limity z ust. 1, z uwzględnieniem limitów maksymalnych dla przelewów natychmiastowych.
8. My decydujemy o ostatecznej wysokości limitów.
9. Przelewy wewnętrzne pomiędzy Twoimi rachunkami nie wliczają się do limitów z ust. 1.

I. Inne postanowienia

§ 34

1. Nie wolno Ci przekazywać przez serwis internetowy bezprawnych treści.
2. Nie możesz wykorzystywać serwisu internetowego do popełniania, pomagania w popełnianiu lub podżegania do popełniania czynów zabronionych. W szczególności dotyczy to wprowadzania do obrotu finansowego wartości majątkowych, które pochodzą 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	19
Rozdział 2. Dyspozycje składane za pośrednictwem elektronicznych kanałów dostępu	21
A. Dyspozycje ogólne	21
B. Autowypłata	24
Rozdział 3. Korzystanie z usług bankowości elektronicznej	25
Rozdział 4. Ograniczenia w korzystaniu z usług bankowości elektronicznej	25
Rozdział 5. Blokowanie i zastrzeganie dostępu do bankowości internetowej	26
Rozdział 6. Udostępnianie informacji na potrzeby świadczenia usług inicjowania transakcji płatniczych i usług dostępu do informacji o rachunku. Potwierdzanie dostępności środków na rachunku	27
Rozdział 7. Aplikacja mobilna Nasz Bank	28
A. Korzystanie z aplikacji mobilnej	28
B. Zasady bezpieczeństwa	29
C. Ograniczenia w korzystaniu z aplikacji mobilnej	30
D. BLIK w aplikacji mobilnej	31
E. Realizacja transakcji dokonywanych w usłudze BLIK	33
F. Usługa smartKARTA w aplikacji mobilnej Nasz Bank	35
G. Realizacja transakcji dokonywanych w usłudze smartKARTA	35
H. Funkcjonalności dostępne w aplikacji mobilnej Nasz Bank	36
Rozdział 8. Standardowe limity pojedynczej transakcji oraz limity wszystkich transakcji w ciągu dnia	38
Rozdział 9. Inne postanowienia	39

Rozdział 1. Udostępnienie i warunki korzystania z elektronicznych kanałów dostępu

§ 1

- Bank może świadczyć 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 pobranej na urządzeniu mobilnym;
 - 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 dostępnych za pośrednictwem bankowości internetowej znajdują się na stronie internetowej Banku.
- 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*.
- 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

¹ Nie dotyczy IBF.

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

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/pełnomocnikiem 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 zapobieżeniu naruszenia indywidualnych danych uwierzytelniających, w szczególności że przyjmuje do wiadomości, że ze względów bezpieczeństwa poszczególnych indywidualnych danych uwierzytelniających nie wolno przechowywać razem ze sobą.
4. Bank zapewnia należyłą 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)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 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.
3. Zgody na wykonanie transakcji płatniczej użytkownik może udzielić również za pośrednictwem dostawcy świadczącego usługę inicjowania transakcji płatniczej.

³ Nie dotyczy IBF.

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 POS⁴;
 - 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 uwierzytelnienia;
 - 4) jeżeli użytkownik inicjuje transakcję płatniczą w sytuacji, gdy płatnik i odbiorca są tą samą osobą fizyczną lub prawną i oba rachunki płatnicze są prowadzone przez Bank,
 - 5) inicjowania 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;

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

- 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) mObywatel⁵;
 - 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) mObywatel⁵;
 - 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 mObywatel⁵ 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 użytkownika. Urządzeniem zaufanym może być, np. prywatny komputer, smartfon lub

⁵ Usługa dostępna po wdrożeniu przez Bank.

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 potwierdzania 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 przesyła 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, 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 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 możliwie krótki okres niezbędny do usunięcia przyczyny ograniczenia lub blokady.

Rozdział 5. Blokowanie i zastrzeganie 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 wydanego przez danego dostawcę, oraz
 - 3) dostawca uwierzył w 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

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) niedostępniania aplikacji mobilnej ani kodu BLIK osobom nieuprawnionym,
 - 6) niedostępniania 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/smartKARTA w aplikacji mobilnej, o ile nie nastąpiło zablokowanie dostępu do aplikacji.
6. Użytkownik może sam, w każdej chwili, zablokować/odblokować usługę BLIK/usługę smartKARTA 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) kodu odblokowującego ekran,
 - 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 nieznanych źródeł i od nieznanych 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, nieznanych 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

§ 23

1. Bank uprawniony jest do czasowego zablokowania usługi BLIK/usługi smartKARTY/aplikacji mobilnej w przypadku:
 - 1) uzasadnionych przyczyn związanych z bezpieczeństwem usługi,
 - 2) stwierdzenia dokonania lub próby dokonania transakcji przez osobę nieuprawnioną,
 - 3) użytkownika usługi w sposób niezgodny z prawem,
 - 4) umyślnego doprowadzenia do nieautoryzowanych transakcji.
2. Bank jest zobowiązany zablokować dostęp do aplikacji, uniemożliwiając tym samym wykonanie dyspozycji, w jednym z następujących przypadków:
 - 1) złożenia przez użytkownika dyspozycji zablokowania lub dezaktywacji aplikacji;
 - 2) 3-krotnego wprowadzenia nieprawidłowego PIN-u do aplikacji.
3. Bank ma prawo częściowo ograniczyć lub zablokować dostęp do aplikacji i/lub czasowo zablokować wykonanie dyspozycji w następujących przypadkach:
 - 1) uzasadnionych przyczyn związanych z bezpieczeństwem, tj.:
 - a) uzyskania informacji w tym podejrzenia, iż dyspozycje w aplikacji składane są przez osoby nieuprawnione,
 - b) zagrożenia przechwycenia danych dostępowych przez złośliwe oprogramowanie,
 - c) wykorzystywania danych dostępowych przez oprogramowanie automatycznie logujące się z dużą częstotliwością,
 - d) wykorzystywania systemów lub rachunków w sposób niezgodny z obowiązującymi przepisami prawa,

- e) wykonywania działań mogących zagrażać bezpieczeństwu systemu i danych w nim przetwarzanych;
- 2) podejrzenia nieuprawnionego użycia aplikacji, zaufanego urządzenia mobilnego, indywidualnych danych uwierzytliających lub umyślnego doprowadzenia do nieautoryzowanej dyspozycji;
- 3) powzięcia informacji o zagrożeniu bezpieczeństwa dyspozycji;
- 4) dokonywania czynności konserwacyjnych aplikacji lub innych systemów teleinformatycznych, związanych z korzystaniem z aplikacji, o czym Bank z wyprzedzeniem poinformuje użytkownika w aplikacji mobilnej;
- 5) dokonywania czynności mających na celu usunięcie awarii, usterek lub nieprawidłowości działania aplikacji lub innych systemów teleinformatycznych związanych z jej obsługą.
4. 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 uwierzytliające.
5. 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.
6. Bank może zablokować dostęp do aplikacji w przypadku wygaśnięcia umów produktowych zawartych przez użytkownika z Bankiem.

§ 24

1. Ze względów bezpieczeństwa wykonywania transakcji, Bank ma prawo wprowadzić kwotowe ograniczenia wysokości limitów transakcji wykonywanych w ramach usługi BLIK/usługi smartKARTA.
2. Dienne 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	

3. Użytkownik może zawnieść o indywidualne limity BLIK, z wyłączeniem limitu globalnego oraz limitów ilościowych.
4. 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

5. 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.
6. Podczas dokonywania wpłaty w bankomatach recyklingowych Bank może zapytać o źródło pochodzenia wpłacanych środków.

D. BLIK w aplikacji mobilnej

§ 25

1. Usługa BLIK to usługa umożliwiająca dokonywanie transakcji BLIK za pomocą aplikacji mobilnej Nasz Bank.

2. Bank udostępnia usługę BLIK użytkownikowi bez konieczności składania dodatkowego wniosku. Aktywacja usługi BLIK odbywa się w aplikacji poprzez jej włączenie w ustawieniach.
1. Z usługi BLIK może korzystać wyłącznie użytkownik, który pobrał na zaufanym urządzeniu aplikację mobilną Nasz Bank.
2. W celu korzystania z usługi BLIK użytkownik powinien łącznie spełnić następujące wymagania:
 - 1) 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 BLIK⁶ – 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 Po udostępnieniu funkcjonalności przez Bank.

- 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 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. 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

⁷ Po udostępnieniu funkcjonalności przez Bank.

⁸ Po udostępnieniu funkcjonalności przez Bank.

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 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:
 - 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,
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 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 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.bszi.com.pl
2) transakcja przy użyciu kodu BLIK	tak	tak	BLIK w IBF w wariantach 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 potwierdzanie 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:
 - 1) 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);
 - 2) 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;
 - 3) potwierdzenia tożsamości pracownika Banku w przypadku kontaktu pracownika z klientem – podczas rozmowy telefonicznej z klientem pracownik Banku wysyła komunikat push ze swoimi danymi;

- 4) 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 wymienialnej 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