УМОВИ

надавання послуг Системи інтернет-банкінгу АТ ІНГ Сілезького Банку (ING Banku Śląskiego S.A.) для власників Рахунку для Біженців

діє з 15 березня 2025 року.

Зміст

1. Загальні положення

§ 1

1. Система інтернет-банкінгу АТ ІНГ Сілезький Банк для власників Рахунку для Біженців є товарною маркою послуги електронного банкінгу, про котрий ідеться у Розпорядженні Міністра Розвитку та Фінансів у справі переліку типових послуг, що пов'язані із платіжним рахунком від 14 липня 2017 р. (далі за текстом: Розпорядження). Згідно Розпорядження, послуга електронного банкінгу полягає у доступі до платіжного рахунку через Інтернет, котра дозволяє перевіряти баланс платіжного рахунку, змінювати ліміти для безготівкових платежів та операцій, що проводяться з використанням дебетової картки або видавати інші розпорядження стосовно рахунку. Система інтернет-банкінгу АТ ІНГ Сілезький Банк для власників Рахунку для Біженців може охоплювати також непов'язані із платіжними рахунками послуги. Далі в Умовах будуть вживатися товарні марки (тобто Система інтернет-банкінгу, Система) для визначення послуги електронного банкінгу.
2. Використані в Умовах терміни та абревіатури означають:
   1) **адреса для електронної кореспонденції –** електронна адреса суб'єкта, котрий користується публічною послугою реєстрованої електронної кореспонденції або публічною гібридною послугою, або кваліфікованою послугою реєстрованої електронної кореспонденції, що описана у законі від 18 листопада 2020 р. «Про електронну кореспонденцію» та котра дозволяє однозначно ідентифікувати відправника або отримувача даних, що пересилаються у рамках цих послуг;
   2) **мобільний додаток –** призначений для мобільних пристроїв додаток Банку. Він являється частиною Системи інтернет-банкінгу і також дозволяє мати до нього доступ після його встановлення на мобільному пристрої користувача. Мобільний додаток може бути доступним у різних версіях та під різними товарними марками, напр. «Додаток Моє ІНГ» (Aplikacja Moje ING) або «Моє ІНГ мобайл» (Moje ING mobile), або інші назви. Перелік мобільних додатків, що призначені для даного типу мобільних пристроїв, їх функціональність, в тому числі види розпоряджень, котрі можна видавати за їх допо могою описує Повідомлення;
   3) **Банк –** Акціонерне товариство ІНГ Сілезький Банк із місцезнаходженням у Катовіцах, вул. Сокольська 34, 40-086 Катовіце, занесений у Реєстр підприємців у Районному суді Катовіце-Схід, VIII Економічний відділ Державного судового реєстру за номером 0000005459, що має статутний капітал у розмірі 130 100 000 польських злотих та сплачений капітал у розмірі 130 100 000 польських злотих, Податковий номер НІП 634-013-54-75, що має міжнародний ідентифікаційний код у системі SWIFT (BIC) – INGBPLPW та електронну адресу: info@ing.pl, котрий підлягає нагляду Комісії фінансового нагляду із місцезнаходженням у Варшаві, вул. Пєнкна 20, 00-549 Варшава, котрий веде на підставі дозволів Комісії фінансового нагляду маклерську діяльність у організаційно-відокремленому Маклерському бюро АТ ІНГ Сілезького банку (Biurze Maklerskim ING Banku Śląskiego S.A.);
   4) **пристрій для зчитування біометричних параметрів –** функція мобільного пристрою, доступ до котрої надається його виробником або виробником встановленого на ньому програмного забезпечення. Він використовується для зчитування біометричних параметрів та їх запису в пристрої з метою створення цифрового ключа користувача, що відповідає цим даним;
   5) **біометричний ідентифікатор –** створений у мобільному пристрої та записаний у ньому в цифровій формі ключ користувача, котрий генерується для одного, обраного біометричного параметру користувача та котрий відповідає унікальному коду, котрий створює Банк. Для прикладу, біометричним параметром може бути відбиток пальця або індивідуальні риси обличчя. Унікальний код є перманентно зв'язаним із логіном користувача. Цей код утворюється після затвердження користувачем методу посвідчення або авторизації розпорядження за допомогою біометричного ідентифікатора. Користувач може відкликати дозвіл на його посвідчення або авторизацію розпорядження за допомогою біометричного ідентифікатора дезактивуючи цей метод у мобільному додатку. Біометричний параметр та вищезгаданий ключ користувача не передаються Банку, а також не записуються ним.
   6) **Розпорядження –** кожна заява, котру подав користувач, платіжне доручення також вважається розпорядженням;
   7) **робочий день** – день, що не є суботою або іншим неробочим відповідно до закону днем;

8) **пароль** – послідовність встановлених користувачем символів. Він використовується для входження в Систему інтернет-банкінгу та для надання ПІН-коду для мобільного додатку. Про кількість та тип символів паролю інформує система під час його створення;

9) **ідентифікатор користувача (котрий також зветься логіном)** – індивідуальний послідовність символів, котра надається користувачу Банком і котрий потрібен для входження користувача у Систему інтернет-банкінгу. Він складається з шести літер і чотирьох довільно вибраних цифр і може бути необхідним для посвідчення користувача;

10) **одноразовий активаційний код** – послідовність довільно обраних Банком літер та цифр. Він потрібен для отримання паролю до Системи інтернет-банкінгу та встановлення телефону для авторизації;

11) **гаряча лінія** – телефонна лінія, що призначена для надавання інформації, ведення маркетингової діяльності, продажу та обслуговування вибраних банківських продуктів і послуг, а також комерційних пропозицій інших суб'єктів, послуги або продукти котрих пропонуються Банком або пов'язані із діяльністю Банку. Перелік дій, що виконуються на гарячій лінії є доступним на таблиці оголошень у відділеннях банку та на інтернет-сторінці Банку;

12) **ключ безпеки** – пристрій, що відповідає стандарту, описаному у Повідомленні, який під'єднується до комп'ютера або мобільного пристрою і використовується у процесі посвідчення або авторизації у Системі інтернет-банкінгу. Автентифікація та авторизація за допомогою цього ключа безпеки можлива, якщо Банк надає доступ до цієї функції**;**

13) **авторизаційний код, код для авторизації (код)** – послідовність цифр або , або інших символів, що використовується для посвідчення користувача, в тому числі під час активації Системи або мобільного додатку, або одноразової авторизації розпорядження, котре видається користувачем, в тому числі платіжних розпоряджень. Цей код генерується Банком, якщо даний вид коду не встановлений користувачем. , або інших символів, що використовується для посвідчення користувача, в тому числі під час активації Системи або мобільного додатку, або одноразової авторизації розпорядження, котре видається користувачем, в тому числі платіжних розпоряджень. Кожного разу, коли Умови дозволяють проводити посвідчення або авторизацію за допомогою біометричного ідентифікатора, а користувач увімкнув метод посвідчення або авторизації за допомогою біометричного ідентифікатора, він є авторизаційним кодом у значенні Умов;

14) **ПІН-код** – багатоцифровий код для входу у мобільний додаток, авторизації розпоряджень або платіжних доручень. Його встановлює і змінює користувач. Під час його встановлення або зміни Банк інформує користувача про необхідну кількість цифр ПІН-коду;

15) **Повідомлення** – видане Банком повідомлення для користувачів Системи інтернет-банкінгу для власників Рахунку для Біженців;

16) **Конвенція** – конвенція від 5 жовтня 1961 р. що скасовує вимогу легалізації закордонних офіційних документів;

17) **список ключів безпеки** – містить всі ключі, які користувач вважає безпечними і які відповідають технічним вимогам, визначеним у Повідомленні. Користувач може редагувати список активованих ключів шляхом додавання або вилучення в/з нього відповідних ключів. Список може містити один або більше ключів;

18) **список довірених браузерів (далі – список браузерів)** – містить всі браузери, які користувач вважає безпечними і які відповідають технічним вимогам, визначеним у Повідомленні, і за допомогою яких він вирішує користуватися інтернет-банкінгом. Користувач може редагувати список браузерів шляхом додавання або вилучення в/з нього відповідних браузерів. Список браузерів може містити один або більше браузерів (максимально 5). Браузер додається до списку в момент виконання входу до інтернет-банкінгу за допомогою веб-браузера. Перед збереженням цього браузера як довіреного Банк може вимагати надання або підтвердження даних чи інформації для встановлення особи користувача. Це може бути також інформація, про яку, наскільки відомо Банку, знає тільки користувач. Такий веб-браузер далі йменується «довірений браузер»;

19) **список довірених мобільних пристроїв (далі за текстом список)** – містить усі мобільні пристрої, котрі користувач визнає безпечними та котрі відповідають вимогам щодо правил безпеки, котрі описані в

Умовах і за допомогою яких приймається рішення щодо користування мобільним додатком. Список може містити один або більшу кількість пристроїв. Мобільний пристрій вноситься у список під час активації на ньому мобільного додатку. Перед тим, як для даного пристрою буде наданий статус довіреного мобільного пристрою, Банк може вимагати вказання або підтвердження даних або інформації з метою встановлення особи користувача. Це можуть також бути такі відомості, котрі на думку Банку, відомі виключно користувачеві. Такі пристрої далі іменуються довіреними мобільними пристроями;

20) **NFC – Near Field Communication (скор. NFC – [анг.])** – стандарт високочастотного радіозв'язку ближнього радіусу дії, який дозволяє бездротовий обмін даними на відстані до 20 сантиметрів;

21) **отримувач** – фізична особа, юридична особа або організаційний суб'єкт, що не є юридичною особою, котрій право надає правоздатність, котра є отримувачем грошових коштів, що являються предметом платіжної операції;

22) **відділення** – група одиниць або відділень, що займаються безпосереднім обслуговуванням клієнта або операційним обслуговуванням Банку;

23) **відділення банку** – місце, де клієнта обслуговує спеціаліст або працівник партнера Банку. Відділенням банку є місце зустрічей, пункт касового обслуговування, пункт продажу. Відділення банку розташовані у відділі або за його межами. Інформація про обсяг обслуговування у даному відділенні банку знаходиться у Переліку дій, що виконуються у відділеннях та на гарячій лінії Банку. Перелік є доступним на таблиці оголошень у відділеннях банку та на інтернет-сторінці Банку;

24) **платник** – фізична особа, юридична особа або організаційний суб'єкт, що не є юридичною особою, якій право надає правоздатність, котра видає платіжне доручення;

25) **повідомлення PUSH/ push** – тип повідомлення, котрий відображається на довіреному мобільному пристрої зі встановленим мобільним додатком. Для того, щоб користувач міг отримувати повідомлення push, він повинен мати увімкнену цю функцію на мобільному пристрої, на котрому встановлено мобільний додаток та дати дозвіл на їх отримання. Операційні системи, для яких Банк передбачає використання push-сповіщень, перелічено у Повідомленні;

26) **кнопка підтвердження** – кнопка, за допомогою якої користувач підтверджує видачу розпорядження. Вона може бути позначена графічними символами або назвами, напр.: «Вишли» (Wyślij), «Затвердь» (Zatwierdź), «Підтвердь» (Potwierdź), «Замов» (Zamów), «Прийми» (Akceptuj). Залежно від розпорядження, вона може бути розміщена у різних місцях Системи інтернет-банкінгу;

27) **пункт продажу** – відділення банку, де клієнта обслуговує працівник партнера Банку. У пункті продажу виконуються банківські дії та фактичні дії, що пов'язані із банківською діяльністю на рахунок Банку партнером Банку або його працівниками;

28) **платіжний рахунок** – це платіжний рахунок у значенні закону про платіжні послуги. Договірні умови, що зобов'язують клієнта і котрі стосуються даного рахунку містять інформацію про те, чи даний тип рахунку, що ведеться Банком, є платіжним рахунком;

29) **ощадно-розрахунковий рахунок** – платіжний рахунок у значенні Умов власників Рахунку для Біженців;

30) **Умови** – ці Умови;

31) **Умови ведення рахунків для індивідуальних клієнтів** – Умови надання АТ ІНГ Сілезький Банк послуг з ведення Рахунку для Біженців;

32) **сильне посвідчення користувача (далі за текстом сильне посвідчення) –** означає процедуру посвідчення, що використовується Банком та вимагається правовими положеннями, котра дозволяє захищати конфіденційність даних та вимагає підтвердження щонайменше двох серед елементів, що належать до категорії: а) виключних знань користувача; б) володіння виключно користувачем деякою річчю або пристроєм або в) параметру користувача. Це підтвердження повинно бути незалежним таким чином, що порушення одного з його елементів не послаблює вірогідності інших. Для того, щоб виконати вищенаведену передумову, підтвердження цих обставин буде вимагати вказання користувачем таких елементів, як, напр.:

а) паролю, або

b) платіжної картки незалежно від її форми, в тому числі такі дані картки, як номер картки, термін дії, або

c) ідентифікаційного або авторизаційного коду, або

d) біометричних параметрів, у тому числі тих, що вказуються на пристроях, котрі мають вбудований інструмент для зчитування, напр. телефон або інший пристрій, що має інструмент для зчитування відбитків пальців або біометричних рис обличчя,

e) використання ключів безпеки або інших відомостей, що підтверджують володіння користувачем певною річчю, пристроєм або параметром. Цей елемент вважається дотриманим також тоді, коли пристрій, що належить користувачу, вважається перевіреним. Перевірку можна провести шляхом дистанційного встановлення Банком технічних параметрів або програмного забезпечення пристрою. Перевіреними пристроями є напр. довірені мобільні пристрої, інші пристрої або предмети, на котрих встановлено видану Банком платіжну картку;

33) **непереборна сила** – незалежна від Банку зовнішня подія, котрій Банк не міг запобігти або котрої не міг передбачити і котра безпосередньо або посередньо призвела до невиконання або неналежного виконання Договору Банком. Непереборною силою вважаємо події, що відповідають наступним ознакам:

a) повінь, землетрус, атмосферні розряди, ураган, смерч, вибух вулкану або інші подібні атмосферні явища,

b) відключення постачання струму постачальником електроенергії з незалежних від Банку причин.

Положення про непереборну силу також застосовуються у разі події, що являється проявом влади держави (напр. міжнародна угода, закон, розпорядження, ухвала уповноваженого органу влади/адміністрації), на підставі котрої дана операція або операції деякого типу/виду, або за участі деяких суб'єктів, або операції проведені протягом визначеного часу не можуть бути виконані Банком. Банк доведе до загального відома факт існування непереборної сили та – якщо це можливо – передбачуваний час тривання такого стану;

34) **Система інтернет-банкінгу, інтернет-банкінг, Система** – товарні марки, що використані в Договорі, Умовах та Повідомленні означають послугу електронного банкінгу для власників Рахунку для Біженців. Система інтернет-банкінгу для власників Рахунку для Біженців призначена виключно для його користувачів і є доступною через пристрої із веб-браузером та доступом до Інтернету чи мобільного додатка. Вона може виступати у різних версіях, котрі можуть мати різні товарні марки, напр.: «Моє ІНГ» (Moje ING) або інші. Окремі, під іншими назвами, версії Системи можуть відрізнятися технічними вимогами;

35) **телефон для авторизації** – номер мобільного телефону користувача, що призначений для отримування авторизаційних кодів або надання послуг, що описані у Договорі або Умовах. Цей телефон може також слугувати отримуванню від Банку інформації або повідомлень. Вони можуть стосуватися напр. безпеки операції або змін Умов, або інших договірних положень. Телефон для авторизації вказується користувачем під час подачі заяви про доступ до Системи або укладання Договору чи отримування паролю до Системи. Користувач може, згідно описаної Банком процедури, змінити номер телефону для авторизації;

36) **платіжна операція/ операція** – ініційована платником або отримувачем внесення, переказ або виплата грошових коштів, що призводить до зміни стану коштів на рахунку;

37) **безконтактна операція** – вид операції, котра здійснюється з використанням безконтактної технології на терміналі приймаючої сторони (термінал в Пункті обслуговування продажу) або банкоматі, що є обладнаним пристроєм для безконтактних платежів;

38) **Договір** – укладений між користувачем та Банком *Договір користування системами електронного банкінгу* для власника Рахунку для Біженців, предметом котрого є надання послуги Системи інтернет-банкінгу. Таким договором є *Договір користування системами електронного банкінгу* для власників Рахунку для Біженців.

Завжди, коли у інших документах, в тому числі договорах та додатках буде йтися про *договір користування системами електронного банкінгу для власника Рахунку для Біженців,* розуміти під цим слід Договір;

39) **унікальний ідентифікатор** – комбінація літер, цифр та символів, що визначається Банком, котра надається платником/ отримувачем з метою однозначної ідентифікації другого учасника (платника/ отримувача) платіжної операції або його рахунку. Умови описують унікальний ідентифікатор для окремих видів операцій. Якщо у Договорі або Умовах не передбачено інакше, унікальним ідентифікатором є номер банківського рахунку отримувача або номер мобільного телефону. Щоб номер мобільного телефону отримувача або уповноваженої діяти від його імені особи був унікальним ідентифікатором він повинен бути заздалегідь пов'язаний із одним номером банківського рахунку отримувача або пов'язаний із отримувачем таким чином, щоб можлива була однозначна ідентифікація цього отримувача. Правила такого пов'язування описані в Умовах;
40) **закон про платіжні послуги, закон –** закон від 19 серпня 2011 р. про платіжні послуги;
41) **посвідчення** – процедура, котра дозволяє Банку встановити особу користувача або термін дії даного платіжного інструменту, що використовується, в тому числі його індивідуальних даних, що використовуються для посвідчення. Умови описують які саме дані або інформація мають подаватися з метою встановлення особи;
42) **мобільний пристрій** – багатофункціональний переносний пристрій з доступом до Інтернету, котрий поєднує у собі функції комп'ютера та/ або мобільного телефону. Список операційних систем для мобільних пристроїв, що призначені для користування мобільним додатком наведений у § 28 абз. 3 Умов, у Повідомленні та на інтернет-сторінці Банку
43) **користувач** – це особа, що є стороною Договору;
44) **Перелік** – перелік дій, що виконуються у відділеннях та на гарячій лінії Банку і котрий містить інформацію про обсяг обслуговування, що ведеться у даному відділенні банку. Перелік є доступним на таблиці оголошень у банківських відділеннях та на інтернет-сторінці Банку, та має інформаційний характер;
45) **платіжне доручення** – волевиявлення платника або отримувача направлене Банку, котре містить розпорядження проведення платіжної операції.

3. Завжди, коли в Договорі йдеться про відділ/ відділення банку у відношенні до даної дії, потрібно під цим розуміти те відділення банку, в котрому проводиться дана дія. Інформація про те, у якому відділенні банку дана дія проводиться знаходиться у Переліку. Перелік розміщується на таблиці оголошень у відділеннях банку та на інтернет-сторінці Банку.
4. Завжди, коли в Умовах йдеться про відділення банку у контексті даної банківської дії, інформація, у якому саме відділенні банку ця дія проводиться, знаходиться у Переліку. Перелік розміщується на таблиці оголошень у відділеннях банку та на інтернет-сторінці Банку.

§ 2

1. В Умовах описані правила, згідно котрих Банк надає послуги Системи інтернет-банкінгу для власників Рахунку для Біженців.
2. Предметом надавання є описані в Умовах послуги Системи інтернет-банкінгу, котрі дозволяють Банку виконувати, за допомогою цієї Системи, фінансові послуги.
3. За допомогою Системи користувач має доступ виключно до послуг, в тому числі рахунків, до котрих він є уповноваженим. Уповноваженою вважається особа, яка має право видавати певне розпорядження згідно окремого договору.
4. Якщо деякі фінансові послуги, що є доступними у системі, будуть пов'язані із ризиком, що виникає із їх особливої специфіки або характеру дії, або оплат, котрі залежать від змін цін на фінансовому ринку, опис такого ризику знаходиться в договорах або умовах (загальних умовах договорів), що стосуються даної послуги. Ризики, що пов'язані із послугами Системи інтернет-банкінгу можуть полягати у порушенні описаних в Умовах правил безпеки, зокрема описаних у розділі 16 правил безпечного користування Системою або ризик передачі доступу до пристроїв або додатків неуповноваженим особам.
5. Система інтернет-банкінгу є доступною протягом 24 годин на добу 7 днів на тиждень. Відповідним для виконання платіжних доручень та інших розпоряджень, що видаються через Систему часом

є центральноєвропейський час (CET) або літній центральноєвропейський час у період його введення і до відміни.

6. Пропозиція укладення Договору, зміст котрого охоплюють Умови, не має обов'язкового характеру, хіба що такий характер виразно зазначений у пропозиції Банку.
7. Існує Банківський гарантійний фонд, котрий діє згідно описаних у законі про цей Фонд правил. Інформаційний аркуш стосовно цього Фонду Банк передає власнику рахунку, згідно окремого договору рахунку. Передача інформаційного аркуша та підтвердження його отримання користувачем, котрий є власником рахунку, може відбутися через Систему.
8. Мовою, котра використовується у відносинах Банку з клієнтом, а також тоді, коли Банк діє від імені іншого суб'єкта у якості посередника, агента або представника є польська мова.
9. Відповідним правом, котре являється основою для відносин між Банком і клієнтом перед укладенням Договору та правом, котре є відповідним для укладення і виконання Договору є польське право (право Республіки Польща).
10. У разі, якщо користувач, котрий виступає стороною Договору є також стороною договору іншого банківського рахунку або стороною інших укладених із Банком або за посередництвом Банку угод, а доступ до цих рахунків, послуг або продуктів відбувається за допомогою Системи інтернет-банкінгу, у справах, що не регулюються цими Умовами застосовуються положення укладених користувачем угод, в тому числі умов.
11. За посередництвом Системи користувач може, якщо правові положення дають таку можливість, здійснити: ідентифікацію та посвідчення на електронній платформі послуг державної адміністрації, авторизацію, що пов'язана із користуванням довіреним профілем та підтвердження довіреного профілю.
12. Використання в інших регулятивних документах, що діють для продуктів і послуг Банку назви «Умови надавання послуг Системи інтернет-банкінгу АТ ІНГ Сілезький Банк» означає ці Умови.
13. Повідомлення не є інтегральною частиною Умов і носить інформаційний характер. Зміна змісту Повідомлення не тягне за собою зміни Умов та не призводить до необхідності відмови від Умов.
14. Банк надає доступ до повного змісту Повідомлення:

    1) у відділеннях банку – на таблиці оголошень,

    2) на інтернет-сторінці Банку.
15. Зміна змісту Переліку не тягне за собою зміни Умов та не призводить до необхідності відмови від Умов. Актуальний зміст Переліку знаходиться на таблиці оголошень у відділеннях банку та на інтернет-сторінці Банку

2. Укладення договору

§ 3

1. Договір укладається на визначений термін.
2. Договір може бути укладений у відділенні банку, що виконує такі дії, при чому Банк залишає за собою право виключення можливості укладання Договорів у окремих відділеннях банку.
3. Договір може укласти клієнт, котрий являється фізичною особою та має повне право та дієздатність.
4. Банк не надає доступу до Системи інтернет-банкінгу для осіб, що визнані повністю або частково недієздатними.
5. У ситуації, коли того вимагають правові положення, Банк, перед тим, як надати доступ користувачеві до деяких зазначених у Повідомленні функцій/ послуг проводить перевірку особи користувача за допомогою пред'явленого ним документу, що посвідчує особу під час його фізичної присутності у відділенні банку. Цей запис не застосовується у ситуації, якщо таку перевірку було проведено під час укладання Договору.

3. Надання доступу до системи

§ 4

1. Під час звернення із проханням надання доступу до Системи або максимум після укладення Договору Банк надає кожному користувачеві логін та передає одноразовий активізаційний або авторизаційний код.
2. Для того, щоб користуватися Системою інтернет-банкінгу користувач спершу повинен її активувати. Активація системи означає встановлення власного паролю, за допомогою якого користувач буде входити у Систему.
3. До моменту надання паролю для входження у Систему необхідним є авторизаційний код, котрий передається СМС-повідомленням, що висилається Банком на вказаний користувачем телефон для авторизації або одноразовий активаційний код, котрий надається у відділенні банку, котре вчиняє цю дію, або поштовим відправленням на вказану користувачем кореспонденційну адресу. Авторизаційний код або одноразовий активаційний код може надаватися в іншій погодженій між Банком і користувачем формі.
4. Термін дії авторизаційного коду може бути обмежений з огляду на безпеку Системи. Стандартний термін дії є обмеженим до часу, протягом котрого триває сесія, тобто часу з'єднання користувача із Банком. Одноразовий активаційний код є дійсним 30 днів, котрі рахуються від дати його замовлення користувачем.
5. Якщо користувач отримав одноразовий активаційний код поштою, він має обов'язок зателефонувати на гарячу лінію з метою підтвердження отримання листа. Якщо користувач не підтвердить у телефонному режимі факту вручення йому одноразового активаційного коду, то він не зможе створити пароль та користуватися Системою.
6. Якщо лист із одноразовим активаційним кодом є пошкодженим або якщо одноразовий активаційний код є нерозбірливим, користувач повинен негайно оформити претензію (рекламацію).

§ 5

1. Банк інформує користувача про спосіб передачі логіну під час укладання Договору або у процесі подання заяви про надання доступу до Системи інтернет-банкінгу.

§ 6

1. Із метою надання паролю до Системи користувач зобов’язаний заповнити відповідну заяву, що знаходиться на інтернет-сторінці Банку. Користувача також можуть попросити встановити пароль для Системи під час подання заяви про надання доступу до Системи інтернет-банкінгу.
2. Із огляду на інформаційну безпеку Системи або безпеку депонованих коштів, Банк може обумовити подання заяви наданням користувачем деяких персональних даних або інформації стосовно даної послуги.
3. Якщо користувач не використав одноразового активаційного коду/ авторизаційного коду протягом терміну його дійсності, він повинен звернутися із проханням до Банку надати його ще раз.

4. Посвідчення користувача

§ 7

1. Користувач входить у Систему інтернет-банкінгу особисто, вживаючи для цього виключно власних даних, котрі посвідчують його особу (напр. логін, котрий видав йому Банк).
2. Посвідчення користувача є необхідним як під час входження у Систему, так і під час видання електронного платіжного розпорядження. Пам'ятаючи про положення, що викладені у абз. 3, 4 та 5 посвідчення користувача під час входження у Систему інтернет-банкінгу складається із наступних дій:
   1) вказання правильного логіну,
   2) вказання паролю у замаскованій формі, що означає подання користувачем довільно вибраних Системою символів, що входять в склад паролю,
   3) а у ситуації, якщо цього вимагає право або це виникає із потреб безпеки, додатково також вимагається подання відповідного авторизаційного коду або підтвердження у мобільному додатку, якщо

користувач має мобільний додаток, або використання ключа безпеки, якщо користувач має активований ключ у списку ключів безпеки

Якщо під час входження користувача у Систему Банк вимагає вказання усіх даних, що згадані у п. 1) – 3), це називається сильним посвідченням. Банк використовує сильне посвідчення тоді, коли цього вимагають правові положення.

3. Посвідчення користувача під час входження у мобільний додаток вимагає вчинення наступних дій на довіреному мобільному пристрої:

1) вказання правильного логіну – під час першого входження,

2) вказання паролю у замаскованій формі – під час першого входження, а під час наступних входжень – подання ПІН-коду,

3) у разі, якщо відповідний мобільний додаток встановлено на мобільному пристрої, що обладнаний приладом для зчитування біометричних параметрів, наступні входження можуть відбуватися за допомогою:

a) біометричного ідентифікатора, якщо користувач обрав такий метод посвідчення,

b) а у ситуації, якщо цього вимагає право або це виникає із потреб безпеки, додатково також може вимагатися вказання відповідного авторизаційного коду, котрий не є біометричним ідентифікатором (напр. СМС-код або ПІН-код).

4) якщо це вимагається законодавством або зумовлено міркуваннями безпеки додатково також використання ключа безпеки, якщо користувач має активований ключ у списку ключів безпеки.

Посвідчення називається сильним посвідченням, якщо під час входження у мобільний додаток, Банк вимагає користування довіреним мобільним пристроєм, а крім того вказання усіх відомостей, про котрі йдеться у п. 1) та 2), або інформації, про котру йдеться у п. 3). Із метою протидії безправним входженням Банк має право вводити додаткові засоби або способи підтвердження користувача під час входження у Систему. Банк може ввести додаткові засоби посвідчення також тоді, коли це буде виникати із правових положень.

4. Автентифікація користувача за допомогою ключа безпеки вимагає від користувача:

1) реєстрації ключа безпеки у системі інтернет-банкінгу,

2) активації ключа безпеки у відділенні банку або по телефону гарячої лінії банку, якщо банк надає таку можливість, а також надання згоди на такий спосіб автентифікації.

5. Пам'ятаючи про абз. 7, з метою вибору методу посвідчення за допомогою біометричного ідентифікатора користувач зобов'язаний спершу:

1) провести активацію або конфігурацію функції зчитування біометричних параметрів на мобільному пристрої згідно рекомендацій виробника пристрою або встановленого на ньому програмного забезпечення,

2) ввести у пам'ять цього пристрою один, власний біометричний параметр, котрий буде основою для створення біометричного ідентифікатора користувача,

3) дати дозвіл на метод посвідчення на основі біометричного ідентифікатора.

6. Якщо Банк буде вважати, що технічні та технологічні рішення, на яких базується функція зчитування біометричних параметрів, котрі використав виробник мобільного пристрою створюють ризик для інформаційної безпеки Банку або його клієнтів, він залишає за собою право відмови у проведенні посвідчення користувача на підставі біометричного ідентифікатора. У такій ситуації посвідчення користувача відбувається згідно правил, що описані у абз. 3 п. 1) та п. 2).

7. У разі, якщо користувач використовує довірений мобільний пристрій Банк приймає, що кожне розпорядження, що було видане за допомогою цього пристрою було видане користувачем внаслідок виконання дій спрощеного посвідчення. На підставі вищенаведеного, у той момент, коли пристрій буде доданий до списку, користувач має обов'язок дотримання особливої, підвищеної старанності під час зберігання такого пристрою та не надавання до нього доступу третім особам. Перелік видів розпоряджень, котрі виконуються Банком на підставі посвідчення користувача, що було проведене шляхом поєднання його особи з мобільним пристроєм, котрий він додав до списку містить Повідомлення.

8. Правильне посвідчення користувача, що було проведене згідно абз. 2 та 3, дає можливість користувачеві мати доступ до інформації про рахунки або інші послуги, доступ до котрих надається в рамках Системи та дозволяє видавати розпорядження щодо тих рахунків, а також продуктів і послуг.

9. Хибне посвідчення користувача під час входження у Систему, котре полягає у тому, що п'ять разів підряд був введений невірний пароль, призводить до автоматичного блокування доступу до Системи. Лічильник хибних спроб залогінення обнулиться після правильного входження у систему.

10. Хибне посвідчення користувача під час входження у мобільний додаток по причині того, що три рази підряд був введений невірний ПІН-код спричиняє його блокування і може призвести до блокування доступу до Системи. Лічильник хибних спроб введення ПІН-коду обнулиться після правильного входження у систему. Надати ПІН-код можна тільки після того, як правильно буде введений пароль у замаскованій формі.

11. У разі, якщо користувач під час входження у мобільну аплікацію використав функцію зчитування біометричних параметрів і не відбулося його посвідчення на підставі біометричного ідентифікатора, входження у мобільний додаток буде можливе після того, як буде поданий правильний ПІН-код або інший авторизаційний код.

5. Здійснення волевиявлення та надання інформації у електронній формі

§ 8

1. На підставі укладеного Договору користувач та Банк можуть за посередництвом Системи інтернет-банкінгу здійснювати волевиявлення та обмінюватися інформацією у електронній формі, що пов'язане із виконанням:

1) банківський дій, або

2) інших дій, згідно статуту Банку.

Під час здійснення цих дій потрібно пам'ятати про те, що по причині постійного розвитку інформаційних технологій окремі функції, доступ до котрих надається через Систему інтернет-банкінгу можуть змінюватися або доступ до них може надаватися в різні терміни. Інформація щодо можливості здійснення в даний момент часу певних волевиявлень або проведення обміну інформацією міститься у Повідомленні.

2. Волевиявленням у електронній формі, що пов'язане із вчиненням дій, про котрі йдеться у абз. 1 п. 1) та п. 2) вважаються такі заяви, котрі пов'язані із появою, виконанням, зміною, відмовою, розірванням або припиненням правовідносин, що стосуються цих дій. Такою заявою є також надання, зміна або відклик повноважень, що були видані з метою здійснення дій, про котрі йдеться у абз. 1 п. 1) та п. 2).

3. Якщо здійснені у електронній формі волевиявлення відповідають правовим вимогам, що передбачені для визнання їх такими, що подані у письмовій формі, то вважається, що вони подані у письмовій формі також тоді, коли така форма вимагається для дійсності правочину. У разі видачі розпорядження, в тому числі такого, для котрого необхідним є дотримання письмової форми, підпис можна поставити у електронній формі, якщо він відповідає вимогам електронної форми, що є рівнозначною письмовій формі згідно відповідних правових положень. Такий підпис у електронній формі може бути поставлений і вважатися кваліфікованим електронним підписом, електронним підписом високого рівня або іншим електронним підписом у значенні універсальних правових положень, в тому числі:

1) у формі передачі другій стороні ідентифікаційних даних користувача або Банку, або

2) інший спосіб, що допускається правом.

4. Якщо правові положення дозволяються вважати даний спосіб авторизації розпорядження підписом у електронній формі, то користувач може поставити такий підпис, здійснюючи тим самим авторизацію. У разі, якщо Банк ставить підпис у електронній формі шляхом передачі другій стороні ідентифікаційних даних, то підпис, що відправляється за допомогою Системи містить ідентифікаційні дані особи, що представляє Банк. Банк та користувач, шляхом волевиявлення, що здійснене за допомогою Системи інтернет-банкінгу можуть, шляхом укладення додатку до договору, що був укладений в електронній

формі, ввести інший спосіб підпису в електронній формі, якщо згідно правових положень підпис у такій формі буде відповідати вимогам письмової форми.

5. Банк і користувач можуть вчинити дію або укласти договір/ додаток до договорів, або подати заяву, що вимагає письмової форми у електронній формі, котра є рівнозначною письмовій формі. Якщо правові положення будуть це дозволяти, Банк та користувач можуть за допомогою Системи подавати інші заяви, що вимагають письмової форми у електронній формі, котра є рівнозначною письмовій формі.
6. У разі, якщо із доступної у Системі інформації, заяви або документу виникає, що волевиявлення або інформація Банку чи клієнта стосується більше, ніж одного розпорядження або більше, ніж однієї заяви чи документу, вважається, що один поставлений у електронній формі підпис стосується усіх виданих розпоряджень або всіх заяв чи документів.
7. Банк відправляє користувачеві кореспонденцію, в тому числі всілякі волевиявлення або інформацію, бланки документів, а також укладені користувачем договори разом із умовами та іншими документами за допомогою Системи інтернет-банкінгу, якщо у універсальних правових положеннях не записано інакше. На кореспонденції, в тому числі волевиявленнях та інформації, що пересилаються Банком може ставитися електронна печатка, електронна печатка високого рівня або інші електронна печатка, про котру йдеться в універсальних правових положеннях.
8. Банк може надати користувачеві можливість вручати Банку кореспонденцію електронним шляхом за допомогою Системи. Із огляду на розвиток інформаційних технологій доступ до окремих типів заяв (кореспонденції), що надається за допомогою Системи, може змінюватися або доступ до них може надаватися у різні терміни. Інформація стосовно можливості подання у даному часі деяких видів заяв (кореспонденції) заміщена у Повідомленні.
9. Банк буде передавати користувачеві електронним шляхом, у тому числі за допомогою Системи, повідомлення, що підтверджують факт укладення певного договору або прийняття розпорядження для виконання.

6. Отримування електронної кореспонденції

§ 9

1. У рамках Системи інтернет-банкінгу Банк надає користувачеві доступ до:
   1) скриньки „повідомлень”, котра слугує для зв’язку між Банком і користувачем,
   2) електронної системи отримування кореспонденції, в якій Банк буде розміщувати зміни договірних положень, котрі згідно з правом повинні передаватися на тривалому носії інформації. Використання в інших регулятивних документах діючої стосовно продуктів та послуг Банку назви «Електронна система отримування кореспонденції» означає цю послугу. Для користувачів у електронній системі отримування кореспонденції Банк буде розміщувати також виписку з рахунку, інформацію про операції по кредитній картці та інші документи, котрі згідно з правом мають передаватися на тривалому носії інформації.
2. Банк не несе відповідальності за наслідки неналежного ознайомлення із документами/ повідомленнями/ кореспонденцією, що були передані за допомогою Системи інтернет-банкінгу. Користувач зобов’язаний ознайомлюватися з повідомленнями, котрі надсилаються йому Банком за допомогою Системи. Вищенаведене не порушує права Банку висилати користувачеві кореспонденцію поштою на вказану користувачем адресу або вручати йому кореспонденцію особисто у відділенні банку, у котрому надаються такі послуги.
3. Від дня, в котрому Банк надав доступ до Електронної системи отримування кореспонденції, зміни в договірних положеннях, котрі згідно з правом мають надсилатися на тривалому носії інформації, Банк буде вручати користувачам, що є стороною Договору за допомогою Електронної системи отримування кореспонденції. Вона дає можливість користувачеві зберігати адресовану йому Банком інформацію таким чином, що існує можливість доступу до неї протягом періоду, що відповідає цілям складення цієї інформації та ознайомлення із нею у незміненій формі. Цей простір є інтегральною частиною Системи та може вступати під різними товарними марками. Доступ до неї не вимагає укладення окремого договору.

4. Користувач буде мати доступ до Електронної системи отримування кореспонденції до моменту розірвання Договору. Перед розірванням Договору користувач може роздрукувати або записати на іншому тривалому носії інформації документи, котрі передав йому Банк за допомогою Електронної системи отримування кореспонденції.
5. Після розірвання Договору Банк надає користувачеві доступ до вмісту Електронної системи отримування кореспонденції через архів документів (далі за текстом: Архів), якщо Банк надає таку можливість, або передасть такому користувачеві вміст цієї системи на іншому тривалому носії інформації.
6. Для входження в Архів користувач повинен надати Банку свою адресу електронної скриньки та номер телефону для авторизації. Ці дані є необхідними для входження користувачем у Архів.
7. Користуючись Архівом користувач повинен дотримуватися правил безпеки, що передбачені Умовами. У разі підозри, що неуповноважена особа отримала доступ до його Архіву, користувач зобов'язаний негайно заблокувати доступ до свого Архіву або змінити дані, що є необхідними для користування Архівом (електронну скриньку, телефон для авторизації).
8. Банк має право заблокувати доступ до Архіву з тих самих причин, що і блокування Системи. Користувач також може сам заблокувати доступ до Архіву.
9. Користувач може видати розпорядження розблокування Архіву або зміни даних для входження в Архів виключно у відділенні банку, що надає таку послугу.
10. Подробиці пов'язані із користуванням користувачем Архівом знаходяться у Повідомленні.

7. Видання розпоряджень, їх авторизація та виконання

§ 10

1. Банк виконує розпорядження тільки такого користувача, котрому він надав логін.
2. Користувач не може видавати за допомогою Системи розпоряджень, що пов'язані із участю в азартних іграх, предметом котрих було б виконання Банком платіжних послуг, хіба що така гра проводиться згідно закону про азартні ігри. Банк має право відмовитися виконувати такі розпорядження.
3. Видання розпорядження через мобільний додаток буде можливе, якщо у момент виконання цієї дії мобільний пристрій знаходиться у списку довірених мобільних пристроїв.
4. Банк має право встановити вартісні та кількісні ліміти для платіжних операцій, що виконуються на підставі платіжних розпоряджень, що проводяться за допомогою Системи інтернет-банкінгу.
5. У разі, якщо вимагають цього правові положення Банк обумовлює виконання розпорядження, у тому числі платіжних доручень, сильним посвідченням користувача. У разі, якщо Банк вимагає, щоб сильне посвідчення користувача було проведене через мобільний додаток, користувач зобов'язаний під час вчинення цієї дії мати довірений мобільний пристрій.

§ 11

1. Банк здійснює платіжні операції після їх авторизації користувачем. Авторизація платіжного розпорядження користувачем означає його згоду на проведення платіжної операції. Згоду на здійснення платіжної операції користувач може також надати за посередництвом отримувача, постачальника отримувача або постачальника, котрий надає послугу ініціювання платіжної операції.
2. Авторизація розпорядження, у тому числі платіжних доручень, що видаються користувачем за допомогою Системи інтернет-банкінгу складається з наступних кроків:
   1) вибір кнопки підтвердження – якщо Банк вважатиме, що дане розпорядження із огляду на потреби безпеки може бути авторизована таким чином, або
   2) вибір кнопки підтвердження у мобільному додатку (мобільна авторизація) – якщо Банк вважатиме, що дане розпорядження має бути авторизоване у мобільному додатку. Такий спосіб авторизації вимагає одночасно фізичного доступу користувача до довіреного мобільного пристрою, на котрому встановлений і активований мобільний додаток, або

3) вказання правильного авторизаційного коду або кодів, у тому числі біометричного ідентифікатора та вибір кнопки підтвердження – якщо Банк вважатиме, що дане платіжне розпорядження, із огляду на правові положення або правила безпеки вимагає авторизації шляхом вказання авторизаційного коду або кодів, або

4) вказання правильного авторизаційного коду або кодів, в тому числі біометричного ідентифікатора та наближення мобільного пристрою до терміналу, або

5) використання ключа безпеки, якщо користувач має активований ключ у списку ключів безпеки, а також якщо Банк вирішить, що таке розпорядження з урахуванням вимог безпеки може бути авторизоване таким чином, або

6) використання фізичної платіжної картки з увімкненим безконтактним платежем шляхом піднесення її до мобільного пристрою з встановленим мобільним додатком та увімкненою функцією NFC.

3. Авторизація розпорядження за допомогою біометричного ідентифікатора спершу вимагає від користувача:

1) активації або конфігурації функції зчитування біометричних параметрів на мобільному пристрої згідно рекомендацій виробника пристрою або встановленого на ньому програмного забезпечення,

2) введення у пам'ять цього пристрою обраного біометричного параметру користувача, котрий буде основою для створення його біометричного ідентифікатора та надання дозволу на додатковий метод посвідчення і метод авторизації розпорядження за допомогою біометричного ідентифікатора.

4. Із огляду на потреби безпеки Банк залишає за собою право відмови проведення авторизації розпорядження, що видане на підставі біометричного ідентифікатора. Причиною цього може бути те, що Банк вирішить , використані виробником мобільного пристрою технічні та технологічні рішення для зчитування біометричних параметрів створюють ризик, що загрожує інформаційній безпеці Банку та його клієнтів. У такій ситуації авторизація розпорядження відбувається згідно правил, що описані у абз. 2, за винятком можливості використання для цієї мети біометричного ідентифікатора.

5. Кожне розпорядження, що видається користувачем і котре має бути виконане Системою і котре буде призводити до зміни стану грошових коштів на рахунках або буде вважатися заявою укладення Банком нового договору або виконання послуги, або буде пов'язане із такою заявою, вимагає авторизації користувачем згідно абз. 2.

6. Авторизація розпорядження за допомогою ключа безпеки вимагає від користувача:
1) реєстрації ключа безпеки у системі інтернет-банкінгу.
2) активації ключа безпеки у відділенні банку або по телефону гарячої лінії банку, якщо банк надає таку можливість, а також надання згоди на такий метод авторизації розпорядження.

7. Застосовуючи правила безпеки Банк перевіряє факт авторизації користувача під час видачі розпорядження шляхом:

1) перевірки правильності даних, що вказані користувачем під час входження у Систему, про котрі йдеться у § 7 абз. 2 і 3,

2) перевірка того, чи користувач натиснув кнопку підтвердження розпорядження, котре було визнане Банком як таке, що не вимагає авторизації шляхом вказання авторизаційного коду,

3) перевірка правильності авторизаційного коду або кодів, що були передані Банком та вказані користувачем, у тому числі біометричного ідентифікатора або верифікація використання ключа безпеки, якщо користувач має активований ключ у списку ключів безпеки.

Якщо результат перевірки, про котру йдеться вище виявиться негативним, Банк вважатиме, що розпорядження не авторизовано користувачем і відмовиться його виконувати.

8. Банк надасть користувачеві авторизаційні коди, котрі є СМС-кодами шляхом відправки СМС-повідомлення на вказаний раніше користувачем телефон для авторизації.

9. Термін дії наданого Банком авторизаційного коду може бути обмеженим із огляду на безпеку Системи. Стандартний термін дії є обмеженим до часу, протягом якого триває сесія, тобто часу з'єднання користувача із Банком через Систему. Авторизаційний код генерується для виданого розпорядження і може бути використаний виключно для авторизації цього розпорядження. Разом із авторизаційним кодом користувач отримує інформацію про подробиці розпорядження.

10. У ситуації, коли п'ять разів підряд буде введений невірний авторизаційний код, що був наданий Банком для затвердження даного розпорядження, доступ у Систему інтернет-банкінгу буде заблокований. У разі, якщо три рази підряд буде введений невірний ПІН-код для затвердження розпорядження у мобільному додатку, Банк може заблокувати доступ у Систему інтернет-банкінгу.

11. Розпорядження щодо розблокування доступу до Системи можна видати у відділенні банку, що надає такі послуги, через інтернет-сторінку Банку, якщо Банк допускає таку функцію. У будь-якому разі, для розблокування користувач повинен надати новий пароль або ПІН-код для мобільного додатку.

12. Із огляду на потреби безпеки, Банк залишає за собою право, вимагати проведення додаткової авторизації, наприклад, за допомогою авторизаційних кодів, ключів безпеки, якщо користувач має активований ключ у списку ключів безпеки.

§ 12

1. Видане користувачем у Системі інтернет-банкінгу розпорядження не можна відкликати і воно є остаточним волевиявленням користувача, при цьому потрібно пам'ятати про зміст абз. 5.

2. Розпорядження, що видаються за допомогою Системи можуть стосуватися виключно рахунків та продуктів або банківських послуг, котрими даний користувач може користуватися за допомогою цієї Системи.

3. Інформація стосовно процесу виконання окремих розпоряджень, що були видані за допомогою Системи інтернет-банкінгу знаходиться у додатку 1 та на інтернет-сторінці Банку, у частині, що стосується Системи.

4. Моментом отримання Банком платіжного доручення, що видане за посередництвом інтернет-банкінгу:

1) у робочий день або в суботу до останньої години, що описана у додатку 1, пам'ятаючи про зміст п. 3), вважається момент проведення авторизації платіжного доручення, про котре йдеться у § 11 абз. 2,

2) у робочий день або в суботу після останньої години, що описана у додатку 1 або у день, котрий згідно закону є вихідним, пам'ятаючи про зміст п. 3), вважається перший робочий день, що йде після дня, в котрому було видане платіжне доручення, за винятком платіжних доручень, що вказані у додатку 1, для котрих не має останніх годин приймання платіжних доручень, для котрих моментом отримання платіжного розпорядження вважається момент, що описаний у п. 1),

3) з відстроченою датою платежу (переказ, виконання котрого починається в інший день, ніж день, в котрому було видане платіжне доручення):

a) вважається день, котрий був вказаний користувачем для зняття коштів із рахунку;

b) якщо вказаний користувачем день, коли мають бути зняті кошти з рахунку, не являється робочим днем (за винятком суботи) вважається, що платіжне доручення було отримане у перший робочий день, що йде після дня, котрий був вказаний користувачем для зняття коштів з його рахунку, за винятком розпоряджень, що описані у п. c),

c) якщо вказаний користувачем день, коли мають бути зняті кошти з рахунку, не являється робочим днем (за винятком суботи), то у разі платіжних доручень, що описані у додатку 1, для котрих не має останніх годин приймання платіжних доручень, моментом отримання таких платіжних доручень Банком вважається день, котрий був вказаний користувачем для зняття коштів із його рахунку;

d) якщо вказаний користувачем день, коли мають бути зняті кошти з рахунку припадає на суботу, то вважається, що платіжне розпорядження було отримане того самого дня, за винятком розпоряджень, що описані у п. e),

e) якщо вказаний користувачем день, коли мають бути зняті кошти з рахунку припадає на суботу, то у разі платіжних доручень, що описані у додатку 1, для котрих існують останні години приймання платіжних доручень, то моментом отримання таких платіжних доручень Банком вважається перший робочий день, що йде після дня, що був вказаний користувачем для зняття коштів із його рахунку.

5. Беручи до уваги зміст абз. 6, користувач не може відкликати платіжного доручення від моменту його отримання Банком, хіба що в інших умовах або окремо укладених договорах вказано інакше.

6. У разі вихідного платіжного доручення, про котре йдеться у додатку 1, користувач може його відкликати до дня і години, що вказані у додатку 1.

7. У разі, якщо платіжна операція ініціюється постачальником, що надає послугу ініціювання платіжної операції або отримувачем чи за його посередництвом, за винятком платіжного доручення із відстроченою датою платежу, що описане у абз. 4 п. 3), платник не може відкликати платіжного доручення після того, як надасть постачальнику послуги ініціювання платіжної операції дозвіл на ініціювання платіжної операції або після того, як виразить отримувачу згоду на здійснення платіжної операції.

§ 13

1. Банк виконує розпорядження, в тому числі платіжне доручення, що було видане за допомогою Системи інтернет-банкінгу згідно правил, що описані в Умовах, а в справах, що ними не регулюються – згідно правил, що передбачені окремими та обов'язковими для користувача нормами, котрі стосуються відповідних рахунків або інших послуг, котрих стосується дане розпорядження.

2. У разі розірвання Договору, видане раніше за допомогою Системи платіжне доручення із відстроченою датою платежу буде виконане згідно виданого користувачем розпорядження.

3. Беручи до уваги зміст абз. 5, Банк відмовляється виконувати розпорядження, у тому числі платіжне доручення по причинах, що вказані у договорі або умовах, котрі стосуються користувача та відносяться до відповідного рахунку, а також розпорядження, котре є:

1) неповним або неправильним по причині вказання невірного унікального ідентифікатора або інших хибних відомостей, котрі є необхідними для виконання даного розпорядження,

2) суперечить іншому виданому розпорядженню,

3) котре не можна виконати по причині недостатніх коштів на рахунку, з котрого має бути виконане,

4) неавторизованим згідно процедури, що описана в Умовах,

5) по інших причинах, котрі конкретно передбачені в Умовах, Договорі або універсальних правових нормах.

Вищенаведене стосується усіх платіжних доручень, в тому числі тих, котрі були розпочаті отримувачем або за його посередництвом.

4. Користувач негайно отримує через Систему повідомлення про відмову виконання доручення. Якщо це буде можливе, то він отримає також інформацію про причини відмови або процедуру спростування помилок, котрі призвели до відмови, хіба що таке повідомлення є недопустимим згідно окремих положень

5. У ситуації, якщо в Банку не буде проведено актуалізації документу, що посвідчує особу, котра видає розпорядження через Систему інтернет-банкінгу, Банк має право відмовитися виконувати платіжне доручення.

6. Банк проводить платіжні операції згідно таких самих правил без огляду на те, чи платіжне доручення було видане користувачем безпосередньо в Банку, чи було ініційоване постачальником послуги ініціювання платіжної операції, хіба що в Умовах записано інакше.

§ 14

Доступ до інформації, що вимагається на підставі законів надається періодично, щонайменше раз на місяць, безкоштовно у Системі – хіба що інакше передбачено окремими регулятивними документами, що стосуються користувача або в Умовах.

§ 15

1. У разі, якщо користувач видає розпорядження, котре являється платіжним дорученням у відділенні банку, що надає такі послуги або через гарячу лінію, то він може, якщо Банк передбачає таку можливість, авторизувати таке розпорядження, подаючи у цьому відділенні або під час розмови на гарячій лінії авторизаційний код, що був отриманий шляхом СМС-повідомлення, котре було вислане Банком на його номер телефону для авторизації.

2. У разі, якщо користувач видає розпорядження, котре не являється платіжним дорученням у відділенні банку, що надає такі послуги або через гарячу лінію, то він може, якщо Банк передбачає таку можливість, видати таке розпорядження, за винятком розпоряджень, для котрих Умови передбачають виключно письмову форму або через Систему інтернет-банкінгу, подаючи у цьому відділенні або під час розмови на

гарячій лінії авторизаційний код, що був отриманий шляхом СМС-повідомлення, котре було вислане Банком на його номер телефону для авторизації. Перелік розпоряджень наводиться у Повідомленні.

3. У разі, якщо банк передбачає таку можливість, користувач може видати розпорядження, котре являється платіжним дорученням або розпорядження, котре не являється платіжним дорученням, а також здійснити їх авторизацію ставлячи у відділенні банку, котре надає таку послугу, підпис на електронному пристрої, згідно ст. 7 абз. 1 Банківського права, подаючи перед цим Банку свої ідентифікаційні дані та після встановлення працівником Банку особи, що подає таку заяву. Документи, на підставі котрих Банк встановлює особу, вказані у Повідомленні для власників рахунків, що описані в Умовах надавання АТ ІНГ Сілезький Банк послуг по веденню Рахунку для Біженців. Електронний пристрій дозволяє фіксувати і утримувати інтегральність змісту заяви, поставленого підпису та дати і часу подачі заяви. У разі, якщо волевиявлення клієнта пов'язане із появою, виконанням, зміною, розірванням або припиненням правовідносин, що поєднують його з Банком та вимагає волевиявлення Банку, Банк ставить підпис у електронній формі шляхом заміщення у його змісті ідентифікаційних даних свого представника, тобто імені і прізвища, а також ідентифікаційного номера працівника.

8. Послуги, що підтримують управління фінансами

§ 16

1. У рамках Системи Банк надає послуги з підтримки управління фінансами (далі за текстом: управління фінансами). Ці послуги мають характер консультацій та порад послуг і зокрема пов'язані зі здійсненням платежів.

2. Із метою надання цих послуг Банк надає доступ до функцій Системи, котрі пристосовані до індивідуальних потреб користувача. Для того, щоб Банк міг здійснювати управління фінансами необхідним є проведення категоризації фінансової інформації та профілювання персональних даних, що стосуються користувача у значенні Розпорядження Європейського Парламенту та Ради (ЄС) № 2016/679 від 27 квітня 2016 р. – загальне розпорядження про захист даних. Профілювання може проводитися тільки у обсязі, що є необхідним для здійснення управління фінансами. Здійснюючи управління фінансами банк Бане не приймає рішень у фінансових справах користувача.

3. Управління фінансами не охоплює консультаційних послуг, управління портфелями, ведення інвестиційних, фінансових аналізів та надання інших рекомендацій у значенні ст. 69 абз. 2 та абз. 4 закону про обіг фінансових інструментів, котрі можуть надаватися Банком на підставі інших договорів/ регулятивних документів, навіть коли вони надаються Системою дистанційно.

4. Управління фінансами здійснюється у формі:

1) інформації або повідомлень про:

a) фінансову термінологію та знання у цих сферах,

b) майбутні платежі, у тому числі такі, що проводяться користувачем періодично та майбутні події або терміни,

c) можливі майбутні платежі користувача, у тому числі такі, що здійснюються періодично,

2) презентація фінансової ситуації користувача шляхом надання інформації про:

a) типи операцій, що здійснювалися ним або відношення операцій до деякої групи або типу операцій,

b) тип або категорію надходжень, витрат або бізнес-партнерів,

5. Інформація, презентації та поради, про котрі йдеться у абз. 4 можуть мати різну графічну та текстову форми.

6. Управління фінансами здійснюється згідно наступних правил:

1) інформація стосовно термінології передається у Системі на постійній основі, а повідомлення про майбутні операції/ події або терміни – не пізніше, ніж за 48 годин до вказаної у Системі операції/ події або терміну,

2) презентації фінансової ситуації надаються за місячний або річний період на підставі проведених або запланованих платежів. Такі презентації можуть також містити інформацію, що була надана

користувачем у Системі або іншими суб'єктами, що діють від імені користувача. Система може надати можливість встановити інші періоди для такої презентації.

7. Управління фінансами є інтегральною частиною Системи, однак у рамках цих послуг окремі їх функції можуть вимагати самостійного увімкнення користувачем.

§ 17

1. За належне ведення управління фінансами Банк несе відповідальність за доведені втрати користувача, пам'ятаючи про зміст абз. 2
2. Банк не відповідає за поставлену користувачем мету, завдання або ліміт витрат, а також за їх виконання чи рівень виконання
3. Банк не несе відповідальності за прийняті користувачем рішення, що пов'язані із управлінням фінансами, у тому числі за рішення стосовно придбання окремих послуг або депонування коштів. Виключення відповідальності не стосується ситуації порушення Банком обов'язку ведення діяльності із належною старанністю, а також не порушує безумовно зобов'язуючих правових норм.
4. Банк готує консультації згідно своєї найкращої волі та знань і з дотриманням належної старанності, на підставі відомого Банку фактичного стану, що існував у момент її надання, а зокрема на підставі наданої користувачем інформації. Банк не перевіряє чи надана користувачем інформація є достовірною. Для отримання вірогідної консультації користувач зобов'язаний надавати правдиві відомості, зокрема стосовно фінансової ситуації.
5. У разі, якщо у рамках управління фінансами дана функція вмикається користувачем самостійно, Банк – незалежно від інформаційних обов'язків, що виникають із правових вимог – може передати додаткову інформацію про ризики, що пов'язані із послугами. Користувач зобов'язаний ознайомитися із такою інформацією та прийняти раціональне рішення щодо депонування коштів.
6. Із огляду на постійний розвиток інформаційних технологій окремі функції, доступ до котрих надається в рамках управління фінансами можуть змінюватися або вмикатися у Системі у різні терміни. Інформація стосовно їх доступності знаходиться у Повідомленні. Ці функції можуть мати різні позначення і назви.
7. Управління фінансами здійснюється до моменту закінчення терміну дії або розірвання Договору. Після цього користувач не має доступу до результатів надання послуг по підтримці управління фінансами, котрі підготував Банк, а зокрема до інформації, презентацій, порад та фінансових цілей або заходів, котрі встановлював користувач. Перед закінченням терміну дії або розірванням Договору користувач може роздрукувати результати фінансових консультацій або записати їх та зберігати на електронному носії – якщо Система надає можливість створення консультації у формі текстового файлу.

9. Електронний сейф у системі інтернет-банкінгу

§ 18

1. Електронний сейф (далі за текстом: сейф) є послугою, котра полягає у зберіганні записаних користувачем електронних документів (що також називаються файлами) у спеціально виділеному просторі Системи інтернет-банкінгу. Цей простір є інтегральною частиною Системи і може виступати під різною товарною маркою.
2. Банк надає доступ до послуги сейфу користувачам, котрі уклали Договір. Користування цією послугою не вимагає укладення окремої угоди. У просторі сейфу користувач може записати файли, взяти або усунути раніше записані ним файли. Користувач не має можливості редагувати записані файли або змінювати їх формати.
3. Каталог форматів файлів, котрі можна записувати у Системі вказаний у Повідомленні.
4. Користувач отримує доступ до сейфу від моменту входження у Систему. Користувач може користуватися сейфом тоді, коли він знаходиться у Системі.
5. Сейф прив'язаний до логіну користувача. Якщо користувач має кілька логінів, то ця послуга є доступною окремо для кожного логіну. Не має можливості користуватися одним і тим же сейфом в рамках кількох логінів.

6. Інформація про доступну ємність сейфу вказана у Системі.

7. Користувач відповідає за зміст записаних файлів та їх формат. Користувач може записувати у сейфі тільки такі файли, щодо котрих має відповідні повноваження, котрі не порушують універсальних норм права, були складені або отримані згідно права та не порушують прав третіх осіб, в тому числі особистих немайнових благ, авторських прав, прав промислової власності, або комерційних таємниць тих осіб. Користувач може записувати тільки такі файли, котрі не містять будь-яких електронних вірусів чи будь-яких частин небезпечного програмного забезпечення.

8. Банк має право відмовитися записувати у сейфі документ користувача, котрий не відповідає технічним вимогам і котрий загрожував би безпеці Банку, електронним системам Банку або іншим користувачам чи коштам, що зберігаються у Банку. Від моменту отримання інформації про порушення положень § 27 абз. 7 Банк відмовляється розміщувати файли користувача. У разі, якщо порушення безпеки або порушення обов'язків, що вказані у абз. 7 могло призвести до значних втрат для Банку або інших користувачів, Банк має право задіяти відповідне безпекове програмне забезпечення, а у разі появи раптового ризику – провести ізоляцію, а якщо це виявиться необхідним – усунути файли, що зберігаються.

9. Банк не має доступу до файлів та документів, що розміщені користувачем у сейфі, не перевіряє та не аналізує даних та змісту, що в них містяться. Банк несе відповідальність, що передбачена Умовами від моменту запису такого файлу в сейфі.

10. Зберігаючи файли, що записані користувачем та дотримуючись належної старанності, Банк не несе відповідальності за:

1) зміст та відомості, що містяться у файлах та документах, котрі розміщені у Системі,

2) зміну назви файлів, котру провів користувач,

3) взяті із сейфу файли від момент видачі розпорядження,

4) наслідки порушення користувачем прав, що описані у абз. 7 або 8,

5) заміщення в сейфі файлу від моменту закінчення терміну дії або розірвання договору про Систему,

6) страти та витрати, що були наслідком будь-яких пошкоджень файлу, повного його пошкодження або перехоплення файлу під час його передачі у Систему, хіба що причиною була функціональність інформаційної системи Банку,

7) не виявлення Банком, під час записування файлу у Системі, чи має він які-небудь елементи, що містять вірус,

8) запізнення під час виконання або невиконання розпорядження користувача стосовно послуг сейфу, якщо це було спричинене непереборною силою.

11. Уповноваженим згідно права органам Банк надасть доступ до вмісту сейфу без проведення аналізу файлів, котрі там зберігаються та згідно процедури, що передбачені відповідними положеннями банківського законодавства.

12. Банк не несе відповідальності за шкоду, що виникає із надання доступу до вмісту сейфу уповноваженим особам або органам, котрі мають право вимагати від Банку надання таких відомостей,

13. Користувач втрачає доступ до сейфу та записаних у ньому файлів/ документів від моменту закінчення терміну дії або розірвання Договору. У момент закриття Системи, файли/ документи, що зберігаються у сейфі автоматично невідворотно усуваються Банком. Банк не зберігає копій таких файлів/ документів. Перед розірванням/припиненням Договору Банк повідомляє користувача про необхідність завантаження записаних файлів. Повідомлення про це може бути надане довільним чином, в тому числі за допомогою повідомлення, котре буде показане користувачеві у Системі.

14. Із огляду на технічні причини, розвиток технології та програмного забезпечення, котре використовується для обслуговування сейфу або для потреб безпеки, Банк має право обмежити можливість користування функцією запису деяких форматів файлів у сейфі або обмежити функціональність сейфу. У такому разі, перед тим, як виконати деяку операцію, користувач отримає к Системі відповідну інформацію.

10. Користування платіжними послугами, котрі надаються уповноваженими третіми суб'єктами

§ 19

1. Користувач може, у обсязі повноважень, котрими він володіє, користуватися платіжними послугами таких третіх суб'єктів, котрі надають послугу доступу до інформації про рахунок або послугу ініціювання платіжної операції:
   1) послуга доступу до інформації про рахунок – надається постачальником послуги доступу до інформації про рахунок і полягає у наданні Банком – на вимогу цього постачальника – інформації про рахунок, котрий ведеться Банком;
   2) послуга ініціювання платіжної операції – надається постачальником послуги ініціювання платіжної операції і полягає у ініціюванні цим постачальником, котрий діє за розпорядженням користувача, платіжного розпорядження із платіжного рахунку, котрий ведеться Банком і до котрого користувач має право.
2. Користування послугою доступу до інформації про рахунок є можливим за умови, що рахунок, котрий ведеться Банком, є платіжним рахунком із доступом он-лайн, а користувач буде посвідчений Банком згідно правових вимог та положень Умов.
3. Користування послугою ініціювання платіжної операції є можливим за умови, що згідно зобов'язуючих користувача регулятивних документів це є електронна безготівкова операція, що стосується платіжного рахунку, до котрого доступ здійснюється он-лайн, її ініціювання відбувається виключно шляхом видачі розпорядження користувачем, а крім того користувач буде посвідчений Банком згідно правових вимог та положень Умов.
4. Постачальнику, котрий надає послугу доступу до інформації про рахунок Банк надає інформацію про визначені рахунки та пов'язані із ними операції, у тому числі історію тих рахунків, однак період, за котрий Банк надає відомості про історію рахунків може бути обмежений по технологічних причинах.
5. Банк не відповідає за належне виконання уповноваженими третіми суб'єктами послуг, про котрі йдеться у абз. 1.
6. Користувач може у Системі дати дозвіл на те, щоб Банк дав відповіді на звернення постачальника платіжних інструментів, що базуються на платіжній картці про те, що сума даної платіжної операції, що проводиться на підставі цієї картки є доступною на платіжному рахунку.
7. Платіжний рахунок є доступним он-лайн, якщо виконані усі наступні передумови:
   1) користувач є стороною Договору,
   2) користувач має активний доступ до Системи інтернет-банкінгу,
   3) даний платіжний рахунок є доступним через Систему в моменті отримання Банком відповідної заяви або вимоги від даного постачальника щодо вчинення дії з метою виконання послуги, про котру йдеться у абз. 1.
8. Платіжний рахунок не є доступним он-лайн, якщо в моменті отримання Банком відповідної заяви або вимоги вчинення дії:
   1) користувач не має активної Системи інтернет-банкінгу, або
   2) якщо доступ у Систему заблокований, або
   3) якщо користувач скористався функцією приховування даного рахунку у Системі та не відкликав цього розпорядження.
9. Банк може відмовитися надати постачальнику послуги доступ до інформації про рахунок або постачальнику послуги ініціювання платіжної операції доступ до даного платіжного рахунку з об'єктивно обґрунтованих та належним чином задокументованих причин, що пов'язані із нелегальним або неуповноваженим доступом до платіжного рахунку, що був здійснений таким постачальником, у тому числі неуповноваженим ініціюванням платіжної операції. У такому разі Банк повідомить користувача через Систему про відмову у наданні доступу до платіжного рахунку та її причинах. Ця інформація, якщо це

можливо, передається користувачеві перед відмовою у доступі, а саме пізніше негайно після такої відмови, однак не пізніше, ніж у робочий день, що є наступним після дня, коли була видана така відмова, хіба що передача такого повідомлення була б нерекомендованою з об'єктивних причин безпеки або суперечить окремим положенням.

11. Відповідальність банку

§ 20

1. Банк зобов'язується:
   1) захищати конфіденційність усіх даних, що використовуються користувачем для посвідчення і авторизації,
   2) надавати, за допомогою Системи інтернет-банкінгу, користувачеві доступ до поточної інформації про рахунки, щодо котрих він має право, таким чином, щоб можливим був постійний моніторинг операції, котрі проводяться на тих рахунках.
2. Банк несе відповідальність за доведені втрати користувача, що спричинені невиконанням розпорядження або його невірним чи невчасним виконанням, хіба що це є наслідком обставин, за котрі Банк не відповідає.
3. Банк несе відповідальність за можливі наслідки виконання операцій третіми особами, після отримання повідомлення, про котре йдеться у § 22a абз. 4 і 5 п. 1) та видачі користувачем розпорядження заблокування доступу у Систему, починаючи від:
   1) надходження розпорядження у Банк – у разі, якщо розпорядження видано через Систему,
   2) письмового підтвердження Банком факту видачі такого розпорядження – у разі, якщо розпорядження видано у відділенні банку, котре надає такі послуги,
   3) отримання користувачем усного підтвердження з гарячої лінії про заблокування доступу до Системи - у разі, якщо розпорядження видано через гарячу лінію.

   - хіба що користувач навмисно здійснив неавторизовану операцію.
4. Банк несе відповідальність за захист конфіденційності даних користувача, котрі використовуються для посвідчення і авторизації за допомогою Системі інтернет-банкінгу тільки у тому випадку, якщо користувач користується цими даними згідно правил, що описані в Умовах, хіба що конфіденційність була порушена по вині Банку.
5. Банк не несе відповідальності за невиконання або неналежне виконання Договору у разі, якщо причиною невиконання або неналежного виконання Договору, у тому числі операції, була непереборна сила.
6. Банк не несе відповідальності за невиконання Договору у разі, якщо відмова у виконанні зобов'язань, що виникають з Договору, видається на підставі положень універсального права, котрі надають Банку право і накладають обов'язок відмовитися виконати такі зобов'язання або розпорядження.
7. Банк не несе відповідальності за:
   1) невиконані розпорядження – у ситуації неправильної або неповної інформації щодо унікального ідентифікатора, або у ситуації, якщо платник чи отримувач не надасть необхідну для виконання даного розпорядження або операції інформацію, у обсязі, в якому невиконання розпорядження виникає з ненадання інформації, що є необхідною для виконання,
   2) наслідки функціонування телекомунікаційних пристроїв користувача, що пов'язані із отримуванням СМС-повідомлень, якщо запізнення у отримуванні повідомлень не сталося по вині Банку,
   3) шкоди користувача, що були заподіяні внаслідок недотримання користувачем правил безпеки Системи інтернет-банкінгу.
8. Стосовно користувачів, котрі являються стороною договору про платіжний рахунок у значенні закону, Банк несе відповідальність за невиконання або неналежне виконання правильно замовленої операції, хіба що він доведе, що на рахунок отримувача надійшли кошти у відповідний з правом термін, або якщо:

1) претензії користувача втратили термін дії внаслідок невнесення протягом 13-місячного терміну, що вимагається
в Умовах, повідомлення про неавторизовані, невиконані або неналежним чином виконані операції, або

2) невиконання або неналежне виконання операції було наслідком непереборної сили або виникало із правових норм.

9. Якщо згідно з Умовами Банк несе відповідальність перед платником або отримувачем, котрий є користувачем, то він зобов'язаний повернути йому суму невиконаної або неналежним чином виконаної операції, а якщо такий користувач є власником платіжного рахунку у значенні закону – повернути рахунок у стан, котрий би існував, якби не сталося неналежне виконання або невиконання операції. Вищенаведене стосується також оплат або відсотків, котрі були накладені на користувача у зв'язку із невиконанням або неналежним виконанням, в тим здійсненим із запізненням виконанням платіжної операції.

10. У разі невиконаної або неналежним чином виконаної платіжної операції, що була ініційована платником або отримувачем, або за його посередництвом Банк, у відповідь на клопотання платника або отримувача, негайно вчиняє дії направлені на безкоштовне відслідковування платіжної операції і – якщо правові положення на це дозволяють – повідомляє платника про їх результат.

11. У справах, що не регулюються цими Умовами, а котрі стосуються відповідальності Банку за виконання платіжних розпоряджень, у тому числі платіжних операцій, котрі були ініційовані за посередництвом постачальника послуги ініціювання платіжної операції та вимог повернення сум неавторизованих операцій стосовно власників ощадно-розрахункових рахунків та ощадних рахунків, застосовуються положення Умов надавання АТ ІНГ Сілезький Банк послуг у рамках ведення Рахунку для Біженців.

12. Під час надавання послуги Системи інтернет-банкінгу згідно положень даних Умов Банк дотримується належної старанності у значенні Цивільного кодексу.

13. Банк не несе відповідальності за безпеку та роботу довіреного мобільного пристрою, у тому числі усіх його функцій.

§ 21

Усі розпорядження, що були видані користувачем у Системі інтернет-банкінгу зберігаються Банком у перманентній формі і являються доказами у разі виникнення спорів.

12. Відповідальність користувача

§ 22

1. При наданні послуг Системи інтернет-банкінгу відповідно до даних Умов Банк проявляє належну ретельність у розумінні Цивільного кодексу.

2. Банк не несе відповідальності за безпеку та роботу довіреного мобільного пристрою, включаючи всі його функції.

§ 22a

1. Користувач зобов'язується не вчиняти жодних дій, які можуть призвести до отримання доступу до Системи третьою особою, навіть якщо це інший користувач

2. Користувач зобов'язаний дотримуватися наступних правил користування Системою:

1) зберігати конфіденційність усіх даних та інформації, що використовуються для:
a) посвідчення та авторизації всіх (платіжних або неплатіжних) розпоряджень (наприклад, логін, коди, пароль, PIN-код), які використовуються для користування Системою або будь-якою її частиною,
b) користування Системою, додатком Моє ІНГ „Aplikacja Moje ING" або будь-якими їхніми функціями чи функціоанльними можливостями.
Ці дані та інформація не повинні розкриватися користувачем третім особам, навіть якщо ця особа є іншим авторизованим користувачем послуг через Систему,

2) запам'ятати свій пароль або інші дані, що використовуються для посвідчення та авторизації, а якщо він не може цього зробити, зберігати цей пароль і дані у безпечний спосіб на свій вибір і в безпечному місці,

недоступному для третіх осіб. Користувач зобов'язаний зберігати пристрої для входу, посвідчення або авторизації (наприклад, ключ U2F) таким же чином. Неприпустимо зберігати пароль і дані, що дозволяють посвідчення або авторизацію, разом в одному місці (наприклад, зберігати пароль разом з іншими даними),

3) користувач зобов'язується не надавати третім особам довірений мобільний пристрій, що дозволило би третім особам отримати дані для посвідчення чи авторизації або надіслати інструкцію до Системи,

4) користувач зобов'язується:

a) не встановлювати та не дозволяти встановлювати будь-яке програмне забезпечення або інструмент на довіреному пристрої або іншому пристрої, який використовує для підключення до Системи, що дозволить третім особам отримати доступ до Системи, та

b) не підключати свій довірений пристрій або будь-який інший пристрій, який використовує для підключення до Системи, до програмного забезпечення, яке дозволить іншим особам/суб'єктам отримати доступ до Системи, в тому числі отримати контроль над пристроєм користувача або керувати його функціями (будь-які способи видачі себе за користувача),

5) користувач зобов'язується захищати довірений пристрій та пристрої, які користувач використовує для підключення до Системи (наприклад, комп'ютер, мобільний телефон, інші мобільні пристрої), від шкідливого програмного забезпечення або доступу третіх осіб шляхом:

a) встановлення на довіреному пристрої та інших пристроях, з яких він підключається до Системи, лише легального програмного забезпечення,

b) встановлення антивірусного програмного забезпечення, з тим, що воно може бути безкоштовним на Довіреному пристрої та інших пристроях, з яких він підключається до Системи,

c) встановлення коду, пароля або PIN-коду або іншого засобу безпеки для доступу до довіреного пристрою або іншого пристрою, з якого користувач підключається до Системи,

d) не допускання зберігання на довіреному або іншому пристрої, що використовується для посвідчення або авторизації, біометричних характеристик третіх осіб, наприклад, рис обличчя (функція face ID) або відбитків пальців, зображень судин (функція touch ID), оскільки це створює ризик того, що пристрій класифікує дані третьої особи як дані користувача,

6) користувач зобов'язаний встановлювати оновлення (в тому числі нові версії та патчі) мобільного додатка на регулярній основі – не пізніше визначених Банком строків. У випадку, якщо оновлення, нова версія або патч є критично важливими, Банк повідомляє користувача про необхідність їх встановлення, впровадження безпосередньо перед входом в систему. Крім того, якщо користувач встановив мобільний додаток або постійно використовує один і той самий пристрій під час користування Системою, користувач зобов'язаний регулярно оновлювати та встановлювати патчі та нові версії, принаймні, програмного забезпечення операційної системи (наприклад, Android, iOS), які рекомендовані виробниками пристроїв або програмного забезпечення, якщо відповідний виробник надає таку підтримку. Неможливість інсталювати поточні версії або патчі у вищезазначеному відношенні може вплинути на безпеку Системи.

3. Користувач повинен дотримуватися наступних правил, що стосуються посвідчення та авторизації інструкцій:

1) перед кожною авторизацією користувач зобов'язаний перевірити, чи відповідає інструкція намірам користувача, а якщо користувач отримує інформацію від Банку перед авторизацією, він зобов'язаний ознайомитися з цією інформацією. Якщо інструкція полягає в додаванні пристрою до списку довірених пристроїв, користувач повинен переконатися, що він є власником пристрою (фактично володіє пристроєм), перш ніж надсилати інструкцію,

2) користувач зобов'язаний негайно повідомити Банк про будь-які несанкціоновані, неправильно ініційовані, невиконані або неналежним чином виконані платіжні операції в результаті інструкцій, поданих з використанням Системи. Таке повідомлення може бути зроблене користувачем через Систему, по телефону на гарячу лінію або у відділенні банку,

3) якщо користувач має намір використовувати метод посвідчення або авторизації на основі біометричного ідентифікатора, він повинен використовувати лише одну власну біометричну характеристику, яка є основою для створення біометричного ідентифікатора. Якщо мобільний пристрій дозволяє реєструвати декілька копій біометричної характеристики (наприклад, відбитки з декількох

пальців), користувач зобов'язаний реєструвати лише одну власну біометричну характеристику, оскільки ця характеристика потім буде призначена ключу користувача, згаданому в § 1, абз. 2, п. 5).

4. Користувач також зобов'язаний негайно повідомити Банк про втрату, крадіжку, привласнення або несанкціоноване використання даних посвідчення або авторизації Системою, а також несанкціонованого доступу до Системи.

5. Користувач також зобов'язаний негайно повідомити Банк у разі виявлення:

1) втрати, крадіжки, незаконного привласнення або виявлення несанкціонованого використання довіреного пристрою або мобільного телефону чи іншого пристрою, який пов'язаний з телефонним номером, позначеним як телефонний номер для посвідчення, або пристроєм для входу в систему, посвідчення або авторизації (наприклад, U2F-ключ),

2) будь-якого технічного інциденту або іншого збою, пов'язаного з використанням Системи, який, на думку користувача, може поставити під загрозу безпеку Системи або безпечне використання Системи користувачем,

3) що треті особи намагалися увійти в Систему. Також існує зобов'язання негайно повідомити Банк, якщо, на думку користувача, існує обґрунтована підозра, що відбулося порушення безпеки або порушення конфіденційності індивідуальних автентифікаційних даних, що використовуються користувачем, таких як коди, коди авторизації або біометричні ідентифікатори.

6. У випадках, зазначених у абз. 4 або абз. 5, а також у разі виявлення або підозри, що відбулося розкриття третім особам даних, які використовуються для посвідчення або авторизації інструкцій, або доступ до Системи іншими особами, користувач повинен негайно:

1) повідомити про це Банк та заблокувати доступ до Системи або доручити Банку блокування доступу до Системи. Доручення на блокування Системи може бути надане у відділенні банку, яке здійснює цю дію, через Систему або через гарячу лінію,

2) змінити всі дані посвідчення або авторизації, які можуть бути змінені.

7. У випадку, якщо користувач виявить, що:

1) було вчинено злочин, в тому числі крадіжку особистих даних, або дію, що призвела до доступу до Системи неавторизованої особи, або

2) третя особа використала інші платіжні інструменти або дані, доступ до яких надається Системою або будь-якою її частиною, або

3) отримання третіми особами біометричних характеристик або біометричних ідентифікаторів, записаних на довіреному мобільному пристрої, може призвести до несанкціонованого доступу таких осіб до мобільного додатка та несанкціонованої авторизації інструкцій, користувач зобов'язаний невідкладно вжити заходів, передбачених абз. 5, та заблокувати відповідні дані або номери платіжних інструментів у відповідних установах. Крім того, у разі підозри на вчинення злочину користувач зобов'язаний повідомити про це компетентний орган, зокрема, прокуратуру або поліцію.

8. Положення про доступ третіх осіб до Системи не стосуються ситуацій:

1) якщо постачальник послуг ініціювання платіжних операцій або постачальник послуг доступу до інформації про рахунок діє від імені користувача, за умови, що ці постачальники діють за згодою користувача з метою та в межах надання цих послуг,

2) якщо іншим користувачем Системи є неповнолітня особа, від імені якої користувач, який є законним представником цієї неповнолітньої особи, уклав договір на користування Системою. Вищезазначене не суперечить принципу, що кожен користувач може надавати інструкції лише самостійно, а неповнолітня особа може давати інструкції лише в тій мірі, в якій вона уповноважена на це своїм законним представником або має на це право згідно із законом.

9. З метою обмеження ризику використання користувачем вебсайтів, подібних до вебсайту Банку, користувач зобов'язаний при вході в систему перевірити, чи є на сторінці, що відображається, сертифікат вебсайту Банку. Спосіб перевірки цього сертифікату є загальнодоступною інформацією та зазначений на

вебсайті Банку та на сторінці входу до Системи Банку. Для інформації надаємо поточну назву вебсайту Банку – www.ing.pl. Назва сайту може бути змінена, про що Банк повідомить в Повідомленні.

10. Користувач не повинен:

1) заходити з довіреного пристрою або будь-якого іншого пристрою, який він постійно використовує під час користування Системою, на вебсайти, які позначені як незахищені або небезпечні (у таких випадках виробники програмного забезпечення також дотримуються практики відображення на пристрої користувача поруч з назвою шуканого вебсайту повідомлення, наприклад, «з'єднання не є безпечним» або знак/позначка «!»),

2) без розбору дозволяти застосункам, встановленим на довіреному пристрої або пристрої, яким користувач користується на постійній основі під час користування Системою, отримувати доступ до інших додатків, а також до своїх фотографій, відео або контактів, – оскільки така практика підвищує ризик несанкціонованого доступу до довіреного пристрою або пристрою, яким користувач користується на постійній основі під час користування Системою.

11. Користувач може надавати повідомлення або сповіщення, про які йдеться в Умовах, через Систему, по телефону на гарячу лінію або в банківській установі.

§ 22b

1. Банк розглядає повідомлення користувача про несанкціоновану операцію, проводячи всебічне розслідування обставин, пов'язаних з цією операцією. Мета розслідування – визначити, чи правильно було подано розпорядженням користувача та чи авторизовано її користувачем. Розслідування також включає визначення того, чи є розпорядження користувача, чи вона була надана третьою особою, також за допомогою програмного забезпечення або іншого пристрою.

2. Якщо з'ясується, що згоди на виконання операції платник не давав, вважається, що така інструкція не була авторизованою. Вищезазначене не порушує правил відповідальності, описаних в цьому Умовах.

§ 22c

1. Якщо користувач порушує одне або кілька зобов'язань, описаних в § 22a, вважається, що користувач не використовує Систему відповідно до Умов.

2. Користувач несе відповідальність за несанкціоновані операції в повному обсязі, якщо вони стали результатом навмисного або виниклого з грубої необережності порушення хоча б одного із зобов'язань користувача відповідно до § 22a, абз. 1-9.

3. За винятком абз. 2, користувач відповідає за неавторизовані операції до розміру суми 50 євро, що розраховується згідно курсу євро, котрий оголошується Національним Банком Польщі (НБП) в день проведення користувачем операції, котрі є наслідком:

1) використання загублених або викрадених даних, що слугують посвідченню та авторизації,

2) незаконного привласнення даних посвідчення або авторизації третьою особою.

Користувач не несе відповідальності за несанкціоновані операції, якщо:

3) не мав можливості довідатися про загублення, викрадення або привласнення даних, що покликані посвідчувати та авторизувати перед здійсненням операції, за винятком ситуації, коли користувач діяв навмисно, або

4) втрата даних, що слугують посвідченню та авторизації перед здійсненням операції була спричинена діяльністю або бездіяльністю з боку Банку або суб'єктів, що вказані у ст. 6 п. 10 закону про платіжні послуги.

4. За винятком ситуацій, описаних у абз. 2 та абз. 3, у разі здійснення неавторизованої операції Банк відшкодовує суму несанкціонованої операції платнику негайно – але не пізніше кінця робочого дня, наступного за днем виявлення несанкціонованої операції або днем отримання повідомлення – за винятком випадків, коли Банк має обґрунтовані та належним чином задокументовані підстави підозрювати шахрайство та письмово інформує про це органи, призначені для переслідування злочинів. Якщо платник користується платіжним рахунком і підлягає поверненню коштів згідно з вищезазначеним правилом, Банк відновлює списаний рахунок до стану, в якому він був би, якби не було здійснено неавторизованої платіжної операції.

5. Платник не несе відповідальності за неавторизовані операції після повідомлення Банку про втрату, крадіжку, привласнення або несанкціоноване використання даних, що використовуються Системою для посвідчення або авторизації, а також про несанкціонований доступ до Системи, як зазначено в § 22a абз. 4, якщо тільки він не діяв навмисно.
6. Якщо операція була неавторизованою і Банк не вимагав від користувача надійної посвідчення, користувач не несе відповідальності за неавторизовану платіжну операцію, за винятком випадків, коли користувач діяв навмисно. Вищезазначене не застосовується, якщо банк мав законне право відмовитися від вимоги надійної посвідчення. Якщо отримувач або постачальник отримувача не приймає надійну автентифікацію користувача, вони несуть відповідальність за завдані Банку збитки.
7. Незважаючи на вищевикладене, якщо користувач не повідомить про неавторизовані, неправильно ініційовані, невиконані або неналежним чином виконані платіжні операції протягом 13 місяців з дати списання коштів з рахунку або з дати, коли операція повинна була бути виконана, вимоги користувача щодо неавторизованих, невиконаних або неналежним чином виконаних платіжних операцій втрачають чинність.

§ 22d

1. Якщо користувач порушує одне або кілька зобов'язань, викладених у § 22 або § 22a, і якщо в результаті цього порушення виявляється, що:
   1) третя особа, використовуючи всі або частину даних посвідчення або авторизації користувача, надала або авторизувала платіжну інструкцію, а Банк виконав цю інструкцію або зробив заяву, що відповідає їй (наприклад, про укладення договору), і
   2) Банк зазнав збитків у результаті виконання інструкції або подання відповідної заяви, оскільки інструкція походила не від користувача,

   то користувач несе відповідальність за відшкодування збитків, завданих Банку внаслідок порушення зобов'язань, передбачених у § 22 та § 22a, відповідно до ступеня порушення цих зобов'язань.
2. Відповідальність користувача обмежується фактичною шкодою, заподіяною Банку внаслідок порушення зобов'язань, передбачених у § 22 та 22a. Відповідальність користувача не виключає права Банку вимагати відшкодування від третьої сторони до повного покриття збитків

13. Інші правила та рекомендації щодо безпечного використання системи

§ 23

1. Банк повідомляє користувача про поточні загрози, тобто спроби шахрайства або підозри їх здійснення, або інші загрози для безпеки користування Системою. Такі повідомлення можуть:
   1) передаватися користувачеві перед тим, як він увійде у Систему,
   2) передаватися користувачеві тоді, як він знаходиться у Системі (напр. після входження, у повідомленнях),
   3) передаватися іншим безпечним каналом комунікації, котрий був погоджений між користувачем та Банком.

   Крім того, інформація у цій справі публікується на інтернет-сторінці Банку.
2. Користувач повинен ознайомитися із повідомленням стосовно загроз, про котрі йдеться у абз. 1 та дотримуватися рекомендацій, котрі в ньому містяться. Якщо він так не чинить, то діє на власний ризик і відповідальність. Неознайомлення із повідомленнями про загрози та недотримання рекомендацій може призвести напр. до:
   1) появи соціотехнічних атак, під час котрих треті особи можуть – видаючи себе за Банк або іншу організацію – схиляти користувача до передачі ідентифікаційних даних, авторизаційних кодів бо ПІН-коду,
   2) авторизації користувачем розпорядження, котрого він не видавав,
   3) використання пристроїв, над котрими контроль перейняли треті особи.

3. Рекомендується, щоб користувач переконався у тому, чи середовище, у якому працює його комп'ютер та мобільний пристрій є безпечним. Користувач зобов'язаний дотримуватися актуальних рекомендацій Банку щодо безпеки операцій, що проводяться через Інтернет з метою захисту від особливих загроз, що виникають з факту з'єднання з Інтернет-мережею. Такі рекомендації подаються Банком на інтернет-сторінці Банку. Інформація про наступні актуалізації таких рекомендацій висилаються Системою.
4. Банк вживає засоби безпеки, котрі зменшують ризик, що пов'язаний із безправним використанням мобільного додатку. У зв'язку із цим Банк має право використовувати електронні механізми, що перевіряють чи користувач або третя особа внесли зміни до довірених мобільних пристроїв або до оригінального програмного забезпечення, котре вимагається його виробником та котре було встановлене на даному пристрої. Вважається, що внесення змін, про котрі йдеться вище може призвести до появи ризику перейняття контролю над пристроєм неуповноваженою особою.
5. Якщо банк встановить, що існує ризик перейняття неуповноваженою особою контролю над довіреним пристроєм, він може знизити операційний ліміт для платіжних доручень, що проводяться за допомогою мобільного додатку встановленого на даному пристрої до 95% суми ліміту, що встановлений в Умовах. Банк негайно повідомить про це користувача. Банк має право заблокувати Систему згідно § 27 абз. 2, якщо ризик, про котрий йдеться вище, зросте до високого рівня або Банк встановить, що за допомогою пристрою, над котрим ймовірно контроль перейняла неуповноважена особа, видаються чергові платіжні розпорядження або інші розпорядження, котрі б могли призвести до неуповноваженого доступу третіх осіб до рахунків, продуктів або послуг за допомогою Системи.

§ 24

1. На інтернет-сторінках та у самій Системі Банк публікує інформацію стосовно безпечного користування Системою. Точні відомості стосовно місця публікації інформації та рекомендацій зі сфери безпеки знаходяться у Повідомленні.
2. Входження у Систему інтернет-банкінгу та користування цією Системою на вимогу користувача вимагає файлів cookie або інших технологій, що походять із цієї Системи. Банк використовує файли cookie та інші технології згідно Політики cookie (далі за текстом Політика cookie). У Системі інтернет-банкінгу файли cookie та інші технології використовуються з метою початку та підтримки сесії користувача у цій Системі, підтримки захисту інтегральності операцій та ідентифікації технічних і технологічних параметрів пристрою, що використовується під час користування послугами Системи, у зв'язку із вимогами безпеки Системи та здійснюваних операцій. У разі, якщо користувач користується інтернет-сторінкою Банку, а не Системою інтернет-банкінгу він може, згідно Політики Банку у сфері файлів cookie, встановити власний веб-браузер так, щоб не затверджувати інших, ніж Системні файлів cookie. Політика cookie, котра використовується Банком є доступною на інтернет-сторінці Банку.
3. Користувач зобов'язаний негайно повідомити Банк про будь-які зміни стосовно персональних та контактних даних користувача. Про зміну даних можна повідомити за допомогою Системи інтернет-банкінгу, якщо у Системі існує технічна функціональність, котра дозволяє таким чином змінити дані. За винятком, коли користувач вручає документ у формі нотаріального акту, власноручність підпису користувача має бути підтверджена:
   1) нотаріусом – у разі документів, що були підписані на території Республіки Польща,
   2) польським дипломатичним представництвом, консульством або нотаріусом країни, з котрою Республіка Польща уклала договір про правову допомогу у цивільних справах, або офіційно чи нотаріально підтверджена разом із доданим апостилем у значенні конвенції – у разі документів, що були підписані за кордоном.
4. За передбаченим у абз. 5 винятком усі розпорядження, що видаються кореспонденційним шляхом, повинні мати форму, що передбачена у абз. 3.
5. Заяви користувачів, зазначені в § 29, абз. 1, § 31, абз. 3, можуть надсилатися кореспонденційним шляхом без дотримання умов, що описані у абз. 3. Банк, однак залишає за собою право проведення додаткової перевірки надісланих заяв.

§ 25

1. Систему інтернет-банкінгу можна розблокувати видаючи розпорядження у відділенні банку, що надає такі послуги, заповнюючи відповідну заяву на інтернет-сторінці Банку або в мобільному додатку, якщо банк допускає таку можливість. Користування Системою буде можливе після того, як буде знову наданий пароль або ПІН-код до мобільного додатку.
2. Користувач може змінити існуючі дані, необхідні для отримання посвідчення або авторизації:
   1) якщо користується тим самим телефоном для авторизації, що і раніше, то може змінити авторизаційні дані за допомогою Системи,
   2) якщо не користується тим самим телефоном для авторизації, що і раніше, то необхідно видати відповідне розпорядження у відділенні банку, що надає такі послуги або подати відповідну заяву на інтернет-сторінці Банку.

§ 26

1. Із метою організації безпеки, мобільний пристрій, на котрому використовуються усі функції мобільного додатку повинен бути доданий до списку довірених мобільних пристроїв. У разі, якщо один мобільний пристрій був вказаний, як довірений кількома користувачами, кожен із цих користувачів повинен дотримуватися вимог щодо безпеки, котрі передбачені Умовами, у тому числі безпечним чином закінчувати користування додатком.
2. Список довірених мобільних пристроїв доступний в Системі.
3. Мобільний пристрій можна усунути зі списку у Системі інтернет-банкінгу або в мобільному додатку. Банк має право усунути мобільний пристрій зі списку, якщо має обґрунтовані сумніви що користувач не користується мобільним пристроєм або доступ до пристрою отримала неуповноважена особа. Вважається, що користувач не користується мобільним пристроєм, якщо він не заходив за його допомогою у мобільний додаток протягом 90 днів. Користувач може знову додати дані пристрою до списку. Із огляду на безпеку, усування і списку – залежно від версії мобільного додатку – може також відбуватися автоматично внаслідок активації додатку на іншому пристрої.
4. Довірений браузер можна вилучити зі списку у Системі інтернет-банкінгу. Банк має право вилучити довірений браузер зі списку, якщо у нього виникнуть обґрунтовані підозри, що користувач не користується цим пристроєм або доступ до пристрою отримала неуповноважена особа. З міркувань безпеки довірений браузер вилучатиметься зі списку через 90 днів із дати його додавання до списку довірених браузерів. Користувач може повторно додати цей браузер до списку.
5. Вилучення ключа безпеки зі списку ключів можливе у Системі банкінгу, якщо попередньо відбулась автентифікація з використанням ключа безпеки або у відділенні банку чи по телефону гарячої лінії банку.
6. У разі загублення, крадіжки, привласнення або встановлення неуповноваженого використання довіреного мобільного пристрою користувач повинен якомога швидше усунути пристрій, котрого стосується підозра, зі списку згідно абз. 3.
7. У разі підозри неуповноваженого використання Системи або крадіжки, привласнення пристрою, з котрим пов'язаний телефон для авторизації або підозри навмисного проведення неавторизованої операції, користувач повинен негайно повідомити Банк за допомогою Системи інтернет-банкінгу або через гарячу лінію.

§ 27

1. Банк залишає за собою право проведення модернізації, актуалізації та регулярних технічних сервісних робіт у Системі інтернет-банкінгу, наслідком чого можуть бути періодичні перерви у доступі до Системи або до деяких його функцій. Про вищезгадані обставини Банк повідомляє, вказуючи планований термін тривалості відсутності або обмеження доступу:

   1) за допомогою опції повідомлень у Системі інтернет-банкінгу та/або

   2) на інтернет-сторінці Банку, та/або

   3) через гарячу лінію.

2. Банк залишає за собою право заблокування доступу до Системи інтернет-банкінгу із огляду на безпеку. Під потребами безпеки потрібно розуміти ситуацію неуповноваженого доступу третіх осіб до банківських рахунків, продуктів або послуг за допомогою Системи або загрозу виникнення такої ситуації, а також у передбачених законодавством ситуаціях.
3. У разі підозри спроби неуповноваженого доступу до Системи Банк може на деякий час вимкнути можливість входу у Систему. Про тривалість такого періоду Банк повідомляє користувача під час входження у Систему.
4. Банк залишає за собою право відмови у виконанні розпорядження або введення додаткових обмежень та забезпечень щодо розпоряджень, котрі видаються через Систему інтернет-банкінгу у разі існування важливих обставин, що не дозволяють виконати таких розпоряджень, тобто перешкод технологічного характеру, із огляду на безпеку або суперечливий зміст розпоряджень та регулятивних документів Банку, котрих повинен дотримуватися користувач, а також у разі недотримання користувачем універсальних правових положень.
5. Банк має право встановити обмеження на використання Системи інтернет-банкінгу у випадку, якщо на підставі місцезнаходження IP-адреси встановить, що Користувач входить до системи в країні, яка входить до переліку країн підвищеного ризику. Перелік таких країн та ступінь обмежень детально викладено на вебсайті Банку.
6. Банк залишає за собою можливість введення обмежень щодо користування із усіх функцій Системи інтернет-банкінгу стосовно деякої групи користувачів, що знаходяться у подібній правовій чи фактичній ситуації. Ці обмеження можуть виникати із потреб безпеки. Про введення обмежень Банк повідомляє користувачів щонайменше за 14 календарних днів до дня введення таких обмежень.
7. Із огляду на безпеку Банк має право вимагати від користувача актуальних персональних даних або підтвердження таких даних.
8. Користувач не має права вписувати або надсилати до Системи змісту, що порушує право, а також використовувати програми, котрі загрожують іншим користувачам Системи або загрожують інтегральності Системи, у тому числі даним, що містяться в ній або в пов'язаному з нею електронному додатку. Якщо ця послуга Системи, в тому числі мобільного додатку, дає можливість відображення даних інших осіб, користувач не має права збирати такі дані, а може їх тільки використати з метою видачі розпорядження проведення платіжної операції.
9. Під час користування Системою Банк може передавати користувачеві інструкції щодо технічно-організаційних інструментів Системи або оголошення про її послуги або функції. Інструкції або оголошення мають виключно інформаційних характер і не являються рекламою. Вони можуть передаватися за допомогою доступних у Системі засобів комунікації або можуть презентуватися напр. у графічній, текстовій, презентаційній або анімаційній формах.
10. Отримання третіми особами біометричних характеристик або біометричних ідентифікаторів, зареєстрованих на довіреному мобільному пристрої, може призвести до несанкціонованого доступу таких осіб до мобільного додатка та несанкціонованої авторизації розпоряджень.
11. Для входу в Систему інтернет-банкінгу та користування нею за запитом користувача використовуються файли cookie або інші технології, що походять із цієї Системи. Банк використовує файли cookie та інші технології відповідно до Політики використання файлів cookie (далі – Політика використання файлів cookie). В Системі інтернет-банкінгу файли cookie та інші технології використовуються для встановлення та підтримки сеансу користувача в Системі, для захисту цілісності операцій та ідентифікації технічних і технологічних характеристик пристрою, що використовується при користуванні послугами Системи, стосовно вимог безпеки Системи та здійснюваних операцій. Якщо користувач використовує вебсайт Банку, але не Систему інтернет-банкінгу, він може, відповідно до Політики Банку щодо файлів cookie, налаштувати власний інтернет-браузер таким чином, щоб він не приймав файли cookie, крім тих, що використовуються в Системі. З Політикою використання файлів cookie Банку можна ознайомитися на інтернет-сторінці Банку.

14. Технічні вимоги користування системою

§ 28

1. Користувач може користуватися Системою за умови виконання наступних, необхідних для співпраці із Системою, мінімальних технічних вимог: мати доступ до електронного пристрою, зокрема такого, як комп'ютер, телефон, інший мобільний пристрій із доступом до Інтернету разом зі встановленими на цьому приладі операційною системою та веб-браузером. У разі наміру користування функціями, що обслуговуються за допомогою інших додатків, напр. мобільного додатку, необхідно встановити даний додаток на мобільному пристрої.
2. Під час дії Договору, користувач повинен вказати телефон для авторизації та користуватися телефоном, відомості щодо котрого він вказував раніше. Ненадання відомостей щодо телефону для авторизації зробить неможливим користування Системою або окремими його функціями.
3. Технічні вимоги, що пов'язані із комунікацією користувача з Системою:

   1) для інтернет-банкінгу – операційна система Apple OS X та Windows

   2) для мобільного додатку – операційна система iOS та Android.

   Додаткова інформація щодо комунікації користувача з Системою або з деякими додатками, програмами, видами файлів або стосовно веб-браузерів та їх версій, а також версій операційних систем подана у Повідомленні та на інтернет-сторінці Банку.
4. У зв'язку із технічним та технологічним розвитком окремі версії Системи – у тому числі мобільні додатки, можуть актуалізуватися, удосконалюватися, змінюватися або замінюватися новими версіями або додатками. Якщо це буде можливо, з технічної точки зору, актуалізації або удосконалення можуть проводитися під час роботи Системи, у тому числі окремих аплікацій. У разі, якщо яка-небудь із вищенаведених операцій вимагатиме від користувача ще раз увімкнути або завантажити нову версію Системи або даного додатку, Банк повідомить його про це за допомогою відповідних екранів, повідомлень або відомостей.
5. Банк може відкликати більш стару версію даного додатку або Системи, замінюючи її більш новою версією. У такому разі користувача заздалегідь повідомляють про плановану дату, коли відбудеться заміна старої версії на нову та можливих необхідних діях, якщо з технічних причин потрібне було б вчинення користувачем якихось дій, зокрема завантаження та встановлення нової версії або вчинення тих дій на даному типі пристрою.

15. Розірвання (одностороннє та за спільною згодою сторін) та закінчення терміну дії договору

§ 29

1. Клієнт має право негайно розірвати Договір без дотримання терміну на повідомлення про такий намір. Розпорядження розірвання Договору може бути видане лише у письмовій формі або за допомогою Системи інтернет-банкінгу, якщо Система дозволяє на такий спосіб внесення заяви про розірвання Договору.
2. Банк має право розірвати укладений з клієнтом Договір із дотриманням двомісячного терміну на повідомлення про такий намір.
3. Банк має право розірвати укладений з клієнтом Договір із дотриманням відповідного та передбаченого вище терміну на повідомлення про такий намір у разі (важливі причини розірвання Договору із дотриманням терміну на повідомлення про такий намір):
   1) встановлення Банком, що користувач не дотримується правил безпечного користування Системою, що описані у розділі 13 Умов,
   2) отримання Банком інформації, що являється обґрунтованою підозрою скоєння користувачем злочину з використанням Системи інтернет-банкінгу або злочину, котрий завдає шкоди Банку,

3) ненадання користувачем описаних в Умовах відомостей, котрі є необхідними для активації даної послуги або необхідними для подальшого надавання послуги Системи інтернет-банкінгу,

4) подання користувачем відомостей або інформації, котрі є фальшивими або невідповідними фактичному стану, у тому числі вживання користувачем недійсних документів (також документів, термін дії котрих закінчився), фальшивих, перероблених або підроблених документів,

5) відсутність можливості виконання Банком обов'язків, що передбачені правилами фінансової безпеки, що описані в законі про протидію відмиванню грошей та фінансовому тероризму.

4. Договір розривається у день смерті клієнта. Факт смерті може бути підтвердженим вірогідним документом, напр.:

1) повним або скороченим витягом зі свідоцтва про смерть,

2) свідоцтво про смерть,

3) засвідчення від органу, що надає соціальну допомогу,

4) відомості з реєстру Загальної електронної системи обліку населення (PESEL),

5) документ від поліції, суду, судового виконавця,

6) іншим вірогідним документом, що підтверджує факт смерті клієнта.

У разі, якщо даний документ викликає сумніви, зокрема щодо його справжності або підтвердження факту або дати смерті користувача, або також існують інші суттєві обставини, що тягнуть за собою сумніви щодо факту або дати смерті користувача, документом, що підтверджує факт смерті Банк буде вважати повний або скорочений витяг зі свідоцтва про смерть, хіба що інша інформація виникає із рішення суду або правових положень.

16. Рекламації. Вирішення спорів

§ 30

1. У справах рекламацій, котрі стосуються платіжних розпоряджень, що передбачені цими Умовами але пов'язаних із рахунками, котрі регулюються відповідно Умовами рахунків для індивідуальних клієнтів застосовуються положення тих умов, котрі є відповідними для даного рахунку. Повноваження щодо умовного зарахування коштів на рахунок або зняття з нього суми, що виникає з рекламації, котрі надані користувачем згідно договору рахунку, стосуються також операцій, що виникають із платіжних розпоряджень, що передбачені цими Умовами. Допоміжна інформація про рахунки, котрі підлягають відповідно під дію Умов рахунків для індивідуальних клієнтів.
2. Подача рекламації на неавторизовані, неправильно ініційовані або неналежним чином виконані чи невиконані розпорядження, котрі були видані через Систему повинна відбутися негайно, однак не пізніше, ніж протягом 13 місяців від дати розпорядження, котре оскаржується.
3. Пам'ятаючи про положення, що містяться у § 22 та § 22a , у разі появи неавторизованої уповноваженою розпоряджатися рахунком особою платіжної операції на рахунку, Банк негайно поверне – однак не пізніше, ніж до кінця робочого дня, що йде після дня виявлення неавторизованої операції, внаслідок котрої були зняті кошти з рахунку платника або після дня отримання відповідного повідомлення, за винятком ситуації, коли постачальник платника має обґрунтовані та належним чином задокументовані підстави, щоб підозрювати шахрайство і повідомить про це у письмовій формі органі, що відповідають за переслідування злочинів – суму неавторизованої платіжної операції та поверне рахунок, з котрого були зняті кошти до стану, який би існував, якби не була проведена неавторизована платіжна операція.
4. Користувач має право подати рекламацію. Рекламація може бути подана:

1) у електронній формі:

a) через Систему інтернет-банкінгу,

b) на адресу електронної кореспонденції, зареєстровану в базі даних електронних адрес AE:PL-69368-51081-ERVRU-12, якщо зареєстрована послуга електронної доставки активована відповідно до чинних правових норм та договорів, укладених між власником депозитного рахунку та банком,

2) в усній формі:

a) по телефону за номерами, вказаними на інтернет-сторінці Банку (вартість дзвінка згідно з тарифами оператора),

b) особисто у відділенні Банку, що надає такі послуги;

3) у письмовій формі:

a) листом надісланим на адресу Банку, що вказана на інтернет-сторінці Банку,

b) особисто у відділенні Банку, що надає такі послуги.

5. У обґрунтованих ситуаціях рекламації, що були подані через Систему інтернет-банкінгу або по телефону гарячої лінії та стосувалися неавторизованих, неправильно ініційованих або неналежним чином виконаних чи невиконаних платіжних операцій або розпоряджень, користувач повинен додатково підтвердити у письмовій формі у відділенні банку, що надає такі послуги протягом 14 календарних днів, котрі рахуються від дати подачі рекламації.

6. Відповідь на рекламацію Банк передає:

1) у електронній формі:

a) через Систему інтернет-банкінгу,

b) на адресу для електронної кореспонденції, що вказана власником, якщо Банк має можливість дати відповідь на ту адресу;

або одним із нижченаведених та вибраним клієнтом способом:

2) у паперовій формі – у відділенні банку або листом на кореспонденційну адресу,

3) на іншому тривалому носії інформації – за згодою сторін.

7. Банк надасть відповідь якомога швидше, однак не пізніше, ніж протягом 15 робочих днів (у разі рекламації стосовно платіжних послуг) та 30 днів (у разі рекламації, котрі не стосуються платіжних послуг), рахуючи від дати її отримання. Під час розгляду рекламації Банк може звернутися по додаткову інформацію або документи. У особливо складних справах, що не дозволяють розглянути рекламацію та надати відповідь у той термін, він може бути продовжений, одна не може перевищити 35 робочих днів (у разі рекламації стосовно платіжних послуг) та 60 днів (у разі рекламації, котрі не стосуються платіжних послуг), рахуючи від дати її отримання. Банк повідомить користувача про причини запізнення, зазначить обставини, котрі потрібно встановити для розгляду рекламації, планований термін закінчення рекламаційного провадження.

8. У ході рекламаційного провадження Банк може звернутися до користувача з проханням надати додаткові пояснення або документи. У разі необхідності з'ясування додаткових у зв'язку із рекламаційним провадженням, що ведеться, Банк залишає за собою право телефонного зв'язку із користувачем за номером телефону, що був вказаний користувачем для зв'язку із Банком.

9. У разі відхилення рекламації Банком користувач має право оскаржити це рішення. Якщо користувачу відомі нові та значимі для справи факти, обставини або докази, він має надати їх Банку у оскарженні. Банк у черговий раз розглядає рекламацію у строки, що вказані для розгляду рекламацій. Якщо у результаті рекламації виникне спір між користувачем та Банком, то він може бути вирішений полюбовно шляхом укладення мирової угоди.

10. Можливі спори, котрі виникають із Договору, котрий уклали Банк і користувач можуть вирішуватися у позасудовому процесі. Клопотання можна заявляти:

1) Фінансовому Речнику, сторінка: www.rf.gov.pl. Речник діє згідно закону про розгляд рекламацій суб'єктами фінансового ринку і про Фінансового Речника та Фонд фінансової освіти;

2) Банківському арбітру, котрий діє в рамках Спілки польських банків, сторінка: www.zbp.pl/dla-konsumentow/arbiter-bankowy/dzialalnosc. Арбітр вирішує спір та видає своє рішення згідно умов банківського споживчого арбітражу.

11. Навіть якщо користувач скористається Платформою ODR він і далі може заявити клопотання Банківському арбітру або Фінансовому речнику. Банк також може заявити клопотання щодо початку позасудового

вирішення спору проти користувача за посередництвом Платформи ODR – якщо обидві сторони раніше погодяться на таке рішення, а умови суб'єкта ADR та законодавство не виключають такої можливості.

12. Користувач може також звернутися по допомогу до речника прав споживача (міського або повітового).

13. Спори, що виникають із Договору можуть також вирішуватися у судовому порядку. Відповідним судом для можливих спорів є суд, що встановлений відповідно положень Цивільного процесуального кодексу.

14. Користувач може подати у орган, що веде нагляд над Банком (Комісія фінансового нагляду) скаргу на дії Банку, якщо згідно точки зору користувача, такі дії порушують правові норми, а також у ситуації відмови надання користувачеві платіжних послуг.

17. Зміни умов

§ 31

1. Банк залишає за собою право внесення змін в Умови з поважних причин. Поважними вважаються такі причини, наслідком котрих є необхідність зміни Умов у потрібному – що виникає із даної причини – обсязі:

1) введення нових або зміна правових положень, що описують правила надання Банком послуг або правила користування такими послугами користувачем,

2) видача органом надзору або іншим уповноваженим органом рішення, рекомендації, поради, точки зору, постанови або іншого документу, що описує правила надавання Банком послуг або правила користування такими послугами користувачем у рамках укладеного з ним договору,

3) розширення, зміна або обмеження функціональності послуг, зміна правил користування послугами користувачем, введення нових послуг, відмова від виконання деяких дій, що являються предметом послуг, котрі надаються Банком у рамках укладеного з користувачем договору.

4) зміни в інформаційній системі Банку, що виникають із:

a) удосконалення інформаційних систем Банку, що спричинено технологічним розвитком,

b) обов'язкових змін, що введені у міжбанківських розрахункових системах стосовно учасників таких систем,

c) змін постачальників програмного забезпечення, внаслідок котрих відбуваються зміни функціональності інформаційної системи Банку.

- котрі мають вплив на послуги, що надаються Банком і котрих стосуються дані Умови або на правила користування такими послугами користувачем у рамках укладеного з ним договору.

2. Про зміни Умов Банк повідомляє користувача погодженим із ним способом, що описаний у § 32 абз. 2 щонайменше за два місяці до пропонованої дати набрання чинності змінами Умов.

3. Користувач має право, перед датою пропонованого набрання чинності змінами:

1) у односторонньому порядку безкоштовно розірвати Договір із юридичним наслідком від дати повідомлення його про зміну, однак не пізніше, ніж до дати, коли такі зміни були б введені в дію,

2) внести протест щодо пропонованих змін.

Якщо перед пропонованою датою набрання чинності змінами користувач не внесе протесту стосовно тих змін, вважається, що він на це погодився. У разі, якщо користувач внесе протест, однак не розірве у односторонньому порядку Договору, Договір припиняє свою дію від дати, що стоїть перед датою набрання чинності пропонованими змінами, безкоштовно.

4. Зміна функціональності Системи або окремих послуг, що спричинена розвитком техніки/ технології не призводить до необхідності зміни Умов, якщо це не призводить до зміни правил надання користувачеві послуг в межах укладеного з ним Договору.

5. Перед пропонованою датою набрання чинності змінами Умов Банк може надати користувачеві можливість користуватися змінами в існуючих послугах або користуватися новими послугами, якщо користувач затвердить зміни Умов стосовно даної послуги.

18. Прикінцеві положення

§ 32

1. Умови доступні у відділеннях банку та на інтернет-сторінці Банку.

2. Банк повідомляє користувача про кожну зміну Умов у формі повідомлення на тривалому носії інформації, що висилається

1) через Систему інтернет-банкінгу, або

2) іншим домовленим між сторонами чином.

3. Назви розділів мають виключно інформаційне значення, що полегшує орієнтування у тексті Умов.

4. Положення набирає чинності з 15 березня 2025 року.

Додатку 1

ПОРЯДОК ВИКОНАННЯ ПЛАТІЖНИХ ДОРУЧЕНЬ ТА ІНШИХ РОЗПОРЯДЖЕНЬ, ЩО ПОДАЮТЬСЯ СИСТЕМОЮ ІНТЕРНЕТ-БАНКІНГУ

Термін подачі платіжних доручень через систему Інтернет-банкінг залежить від годин роботи систем Банку, як показано в таблиці нижче. Платіжне доручення, подане через систему Інтернет-банкінг після кінцевого часу, вважається за отримане у перший робочий день після цього дня.

Порядок виконання платіжних доручень, пов'язаних з переказом, постійного платіжного доручення:

Термін подачі платіжних доручень	**Тип платіжного доручення**	
	Поточний	**Відкладений** <u>незалежно від часу оформлення замовлення</u>
відсутність виконання доручення в режимі реального часу	Доручення, які не потребують конвертації валюти	
	a) доручення внутрішнього переказу в злотих або переказ у рамках послуги «Płać z ING», b) доручення внутрішнього переказу в іноземних валютах, c) зроблений як терміновий переказ Express ELIXIR або BlueCash	a) доручення внутрішнього переказу в злотих b) доручення внутрішнього переказу в іноземних валютах c) постійне доручення на банківські рахунки
відсутність доручення виконується згідно з графіком клірингових сесій банку	Доручення, які не потребують конвертації валюти	
	a) внутрішній переказ, у тому числі переказ, здійснений в рамках послуги «Płać z ING».	a) внутрішній переказ b) постійні доручення на рахунки в інших банках
15:00 (з понеді по п'ятницю)	Доручення, які вимагають і не вимагають конвертації валюти	
	a) переказ системою TARGET	a) переказ системою TARGET
17:00 (з понеділка по п'ятницю)	Доручення, які не потребують конвертації валюти	
	a) переказ іноземної валюти за межі країни b) SEPA-переказ c) доручення на переказ в іноземній валюті	a) переказ іноземної валюти за межі країни b) SEPA-переказ c) доручення на переказ в іноземній валюті
	Доручення, які потребують конвертації валюти	
	a) внутрішній переказ b) переказ іноземної валюти за межі країни c) SEPA-переказ d) доручення на переказ в іноземній валюті	a) внутрішній переказ b) переказ іноземної валюти за межі країни c) SEPA-переказ d) доручення на переказ в іноземній валюті
19:00 (з понеділка по п'ятницю)	Доручення, які потребують конвертації валюти	
	a) доручення внутрішнього переказу в злотих b) доручення внутрішнього переказу в іноземних валютах	a) доручення внутрішнього переказу в злотих b) доручення внутрішнього переказу в іноземних валютах

СКАСУВАННЯ ПЕРЕКАЗІВ, ЗДІЙСНЕНИХ СИСТЕМОЮ ІНТЕРНЕТ-БАНКІНГ

Тип переказу, який можна скасувати – з поточною датою виконання	Коли можна скасувати переказ
системі Інтернет-банкінг користувача може скасувати переказ з ощадних та розрахункових рахунків, поданих цією системою, за винятком переказів з поточною датою виконання, ініційованих провайдером, який надає послугу ініціювання платіжної операції.	
• внутрішній переказ, який не потребує конвертації валюти та не здійснюється в режимі реального часу та не подається як переказ за умовами «Płać z ING	• зроблений **з 00:01 до 8:15 з понеділка по п'ятницю**, його можна скасувати до 9:00 в день здійснення переказу • зроблений **з 8:16 до 11:35 з понеділка по п'ятницю**, його можна скасувати до 13:00 в день здійснення переказу • зроблений **з 11:36 до 14:45 з понеділка по п'ятницю** його можна скасувати до 15:30 в день здійснення переказу • зроблений **з 14:46 до півночі з понеділка по п'ятницю**, його можна скасувати до 9:00 наступного робочого дня • зроблений **з 00:01 до 24:00 у суботу, неділю або у святковий день Банку** , його можна скасувати до 9:00 наступного робочого дня
• переказ системою TARGET • внутрішній переказ, який вимагає конвертації валюти • переказ іноземної валюти за межі країни • SEPA-переказ • доручення на переказ в іноземній валюті	• зроблений **з 17:01 до 24:00з понеділка по п'ятницю,** його можна скасувати до початку наступного робочого дня (до 00:00) • зроблений **з 00:01 у суботу, неділю або у святковий день,** його можна скасувати до початку наступного робочого дня (до 00:00)
• внутрішній переказ, який вимагає конвертації валюти	• зроблений **з 19:01 до 24:00 з понеділка по п'ятницю,** його можна скасувати до початку наступного робочого дня (до 00:00) • зроблений **з 00:01 у суботу, неділю або у святковий день,** його можна скасувати до початку наступного робочого дня (до 00:00)

Ми повернемо кошти від скасованого переказу на рахунок не пізніше наступного робочого дня.