Положения и условия

предоставления услуг системы Интернет-банкинга ING Bank Śląski S.A. для владельцев Счета для беженца

вступившие в силу с 15 марта 2025 г.

Содержание

1. Общие положения

§ 1

1. Система Интернет-банкинга ING Bank Śląski S.A. для владельцев Счета для беженца является торговым названием электронной банковской услуги, упомянутой в Постановлении Министра развития и финансов о перечне представительских услуг, связанных с платежным счетом, от 14 июля 2017 года. (далее: Постановление). Согласно Постановлению, услуга Интернет-банкинга заключается в доступе к платежному счету через Интернет, что позволяет проверять баланс платежного счета, изменять лимиты на безналичные платежи и операции с дебетовой картой или подавать другие виды распоряжений к счету. Система Интернет-банкинга ING Bank Śląski S.A. для владельцев Счета для беженца может также включать услуги, не связанные с платежными счетами. Далее в Положениях и условиях для обозначения электронной банковской услуги будут использоваться торговые названия (например, Система Интернет-банкинга, Система).
2. Термины и сокращения, используемые в Положениях и условиях, означают:
   1) **адрес для электронной доставки –** электронный адрес субъекта, использующего публичную услугу зарегистрированной электронной доставки или публичную гибридную услугу или квалифицированную услугу зарегистрированной электронной доставки, как описано в Законе от 18 ноября 2020 года «Об электронной доставке», позволяющий однозначно идентифицировать отправителя или получателя данных, отправленных в рамках этих услуг;
   2) **мобильное приложение** – приложение Банка, разработанное для мобильных устройств. Оно является частью системы Интернет-банкинга и обеспечивает доступ к ней после установки на мобильное устройство пользователя. Мобильное приложение может быть доступно в различных версиях и под различными торговыми названиями, среди прочего: «Приложение Мой ING» или «Мой ING mobile» или под другими названиями. Перечень мобильных приложений, предназначенных для данного типа мобильных устройств, объем их функциональных возможностей, включая типы распоряжений, которые могут быть поданы с их помощью, описаны в Объявлении;
   3) **Банк –** ING Bank Śląski Spółka Akcyjna с местонахождением в городе Катовице по ул. Сокольска, д. 34, 40-086 г. Катовице, занесенное в реестр предпринимателей Районного суда Катовице-Всхуд, 8-й хозяйственный отдел Национального судебного реестра под номером KRS 0000005459, с уставным капиталом 130 100 000 злотых и оплаченным капиталом 130 100 000 злотых, NIP 634-013-54-75, с международным идентификационным кодом SWIFT (BIC) – INGBPLPW и адресом электронной почты: info@ing.pl, под надзором польского Управления финансового надзора с местонахождением в г. Варшаве, ул. Пенкна, д. 20, 00-549 г. Варшава, осуществляющее на основании разрешений польского Управления финансового надзора брокерскую деятельность в организационно выделенном Брокерском офисе ING Bank Śląski S.A;
   4) **считыватель биометрических признаков –** функция мобильного устройства, предоставляемая его производителем или производителем установленного на нем программного обеспечения. Он используется для считывания биометрических характеристик и хранения их в устройстве с целью создания соответствующего цифрового ключа пользователя;
   5) **биометрический идентификатор –** созданный в мобильном устройстве и хранящийся в нем в цифровом виде ключ пользователя, сгенерированный по одной конкретной биометрической характеристике пользователя и соответствующий уникальному коду, созданному Банком. Например, биометрическим признаком может быть отпечаток пальца или отдельные черты лица. Уникальный код навсегда связан с логином пользователя. Этот код создается после принятия пользователем метода аутентификации или авторизации распоряжения с биометрическим идентификатором. Пользователь может отозвать свое согласие на аутентификацию или авторизацию распоряжений с помощью биометрического идентификатора, отключив этот метод в мобильном приложении. Биометрическая характеристика и вышеупомянутый ключ пользователя не предоставляются Банку и не хранятся им.

6) **распоряжение –** любое заявление, сделанное пользователем, платежное поручение также является распоряжением;
7) **рабочий день –** день, отличный от субботы или праздничного дня;
8) **пароль –** последовательность символов, которую задает пользователь. Он используется для входа в систему Интернет-банкинга и для присвоения PIN-кода в мобильном приложении. Количество и тип символов пароля указывается системой во время его установки;
9) **идентификатор пользователя (также называемый логином)** – индивидуальная строка символов, присвоенная пользователю Банком, которая используется для входа пользователя в систему Интернет-банкинга, в том числе в мобильное приложение. Состоит из шести букв и четырех случайных цифр и может потребоваться для аутентификации пользователя;
10) **одноразовый код активации –** последовательность букв и цифр, генерируемая Банком случайным образом. Он используется для присвоения пароля к системе Интернет-банкинга и определения номера телефона для авторизации;
11) **телефон доверия –** телефонная линия, предназначенная для предоставления информации, проведения маркетинговых кампаний, продажи и обслуживания отдельных банковских продуктов и услуг, а также коммерческих предложений других организаций, услуги или продукты которых предлагаются Банком или связаны с деятельностью Банка. Перечень мероприятий, проводимых по телефону доверия, размещается на доске объявлений в отделениях банка и на веб-сайте банка;
12) **ключ безопасности** – устройство, отвечающее стандарту, описанному в Объявлении, подключаемое к компьютеру или мобильному устройству, используемое в процессе аутентификации или авторизации в Системе Интернет-банкинга. Аутентификация и авторизация с помощью этого ключа безопасности возможны, если Банк предоставит доступ к данной функции**;**
13) **код авторизации, код для авторизации (код)** – последовательность цифр, букв или иных символов, которая используется для аутентификации пользователя, в том числе при активации Системы или мобильного приложения, или для однократной авторизации распоряжений, предоставленных пользователем, в том числе платежные распоряжения. Этот код также может потребоваться для доступа к Системе, включая мобильное приложение или устройство, или для отправки распоряжения. Код генерируется банком, если только определенный тип кода не задан пользователем. Типом кода авторизации может быть, например, SMS-код, PIN-код, код, передаваемый голосом во время автоматического телефонного звонка. Если Положения и условия разрешают аутентификацию или авторизацию с помощью биометрического идентификатора и пользователь включил метод аутентификации или авторизации с помощью биометрического идентификатора, это является кодом авторизации в смысле Положений и условий;
14) **PIN-код –** многозначный код для входа в мобильное приложение, авторизации распоряжений или платежных распоряжений. Он устанавливается и изменяется пользователем. При его установке или изменении банк информирует пользователя о необходимом количестве цифр в ПИН-коде;
15) **Объявление –** объявление, выданное Банком пользователям Системы Интернет-банкинга для владельца Счета для беженца
16) **Конвенция –** Конвенция от 5 октября 1961 года, отменяющая требование легализации иностранных официальных документов;
17) **список ключей безопасности** – содержит все ключи, которые пользователь считает безопасными и которые отвечают техническим требованиям, определенным в Объявлении. Пользователь может редактировать список активированных ключей путем добавления или удаления в/из него соответствующих ключей. Список может содержать один или несколько ключей;
18) **список доверенных браузеров (далее – список браузеров)** – содержит все браузеры, которые пользователь считает безопасными и соответствующими техническим требованиям, изложенным в Объявлении, и с помощью которых он решил пользоваться Интернет-банкингом. Пользователь может изменять список браузеров, добавляя или удаляя из него отдельные браузеры. Список браузеров может содержать один или несколько браузеров (не более 5). Браузер указывается при входе в

Интернет-банкинг через веб-браузер. Банк может потребовать предоставления или подтверждения данных или информации для подтверждения личности пользователя, прежде чем зачислить данный браузер в число доверенных. Это также может включать такую информацию, которая, насколько известно Банку, известна только пользователю. Такой веб-браузер далее называется «доверенный браузер»;

19) **перечень доверенных мобильных устройств (далее – перечень)** – содержит все мобильные устройства, которые пользователь считает безопасными, соответствующими правилам безопасности, изложенным в Положениях и условиях, и с помощью которых он решил использовать мобильное приложение. Перечень может включать одно или несколько устройств. Мобильное устройство попадает в перечень, когда на нем активировано мобильное приложение. Перед тем как зачислить устройство в число доверенных мобильных устройств, Банк может потребовать от пользователя предоставить или подтвердить данные или информацию для идентификации личности пользователя. Это также может включать такую информацию, которая, насколько известно Банку, известна только пользователю. Такое устройство далее называется доверенным мобильным устройством;
20) **NFC** – Near Field Communication (аббревиатура NFC – [англ.] связь ближнего действия) – стандарт высокочастотной радиосвязи малого радиуса действия, позволяющий осуществлять беспроводной обмен данными на расстоянии до 20 сантиметров
21) **получатель –** физическое лицо, юридическое лицо и организационная единица, не являющаяся юридическим лицом, но наделенная законом правоспособностью, являющаяся получателем денежных средств, являющихся предметом платежной операции;
22) **филиал –** объединение подразделений или точек, занимающихся непосредственным обслуживанием клиентов или операционным обслуживанием в Банке;
23) **банковское отделение –** место, где клиента обслуживает специалист или сотрудник банка-партнера. Отделение банка — это место встречи, пункт кассового обслуживания или точка продаж. Банковские отделения располагаются как внутри, так и снаружи филиала. Информация об объеме услуг, предоставляемых в том или ином банковском отделении, содержится в Перечне видов деятельности, осуществляемых в банковских отделениях, и в Информационном центре Банка. Перечень размещен на доске объявлений в отделениях Банка и на веб-сайте Банка;
24) **плательщик –** физическое лицо, юридическое лицо и организационная единица, не являющаяся юридическим лицом, но наделенная законом правоспособностью, которая подает платежное поручение;
25) **PUSH-уведомление/push –** тип сообщения, которое отображается на доверенном мобильном устройстве с установленным мобильным приложением. Для того чтобы получать push-уведомления, пользователь должен иметь включенную функцию на мобильном устройстве, на котором установлено мобильное приложение, и должен дать согласие на их получение. Операционные системы, для которых Банк предусматривает push-уведомления, указаны в Объявлении;
26) **кнопка акцепта** – кнопка, с помощью которой пользователь подтверждает отправку распоряжения. Она может быть обозначена графическими знаками или названиями, например, «Отправить», «Утвердить», «Подтвердить», «Заказать», «Принять». В зависимости от распоряжения, она может быть размещена в различных местах системы Интернет-банкинга;
27) **точка продаж –** банковское отделение, в котором клиента обслуживает сотрудник партнера Банка. В торговой точке банковские действия или фактические действия, которые связаны с банковской деятельностью для Банка, осуществляются партнером Банка или его сотрудниками;
28) **платежный счет –** означает платежный счет в значении Закона «О платежных услугах». В обязательных для клиента договорных положениях и условиях, которые применяются к данному счету, содержится информация о том, является ли данный вид счета, обслуживаемого Банком, платежным счетом;
29) **сберегательный и расчетный счет –** платежный счет в значении Положений и условий для владельцев Счета для беженца,

30) **Положения и условия –** настоящие Положения и условия

31) **Положения и условия счетов для индивидуальных клиентов –** Положения и условия оказания услуг ING Bank Śląski S.A. в рамках ведения Счета для беженца;

32) **строгая аутентификация пользователя (называемая строгой аутентификацией)** – означает процедуру аутентификации, применяемую Банком и требуемую законом, которая обеспечивает защиту конфиденциальности данных и требует подтверждения как минимум двух из элементов, относящихся к следующим категориям: a) исключительное знание пользователя b) исключительное владение пользователем определенным предметом или устройством, или c) характеристика пользователя. Это подтверждение должно быть независимым таким образом, чтобы нарушение одного из его элементов не подрывало надежность остальных. Согласно вышеуказанному правилу, подтверждение этих обстоятельств потребует от пользователя предоставления таких элементов, как:

a) пароль, или

b) платежная карта в любой форме, включая данные карты, такие как номер карты, дата окончанияр срока действия, или

c) идентификационный или авторизационный код, или

d) биометрические признаки, включая признаки, предоставляемые устройствами, содержащими считыватель отпечатков пальцев, такими как телефон или любое другое устройство со считывателем отпечатков пальцев или биометрические признаки лица,

e) использование ключей или другой информации, подтверждающей владение пользователем конкретным предметом, устройством или характеристикой. Этот элемент также считается выполненным, если устройство пользователя считается проверенным. Проверка может осуществляться путем дистанционного определения Банком аппаратных или программных характеристик устройства. Проверенные устройства – это, например, доверенное мобильное устройство, другие устройства или вещи, на которых установлена эмитированная Банком платежная карта;

33) **форс-мажор –** независимое от Банка внешнее событие, которое Банк не мог предотвратить или предвидеть и которое прямо или косвенно привело к неисполнению или ненадлежащему исполнению Договора Банком. Мы считаем форс-мажорными обстоятельствами события, отвечающие вышеуказанным предпосылкам, такие как:

a) наводнение, землетрясение, молния, ураган, торнадо, извержение вулкана или другие подобные атмосферные явления,

b) отключение электроэнергии поставщиком электроэнергии по независящим от Банка причинам.

Положения о форс-мажоре применяются также в случае действия, являющегося суверенным актом государства (например, международным договором, законом, постановлением, распоряжением, решением уполномоченного органа/администрации), в соответствии с которым данная сделка или сделки определенного вида/типа или с определенными субъектами или сделки в определенное время не могут быть осуществлены Банком. Банк обнародует факт наступления форс-мажорных обстоятельств и, по возможности, ожидаемую продолжительность форс-мажорных обстоятельств;

34) **Система Интернет-банкинга, Интернет-банкинг, Система** – торговые названия, которые при использовании в Договоре, Положениях и условиях и Сообщении означают электронную банковскую услугу для владельцев Счета для беженца. Система Интернет-банкинга для владельцев Счета для беженца предназначена исключительно для его пользователей и доступна через устройство с Веб-браузером и Интернет-соединением или мобильное приложение. Она может быть представлена в разных вариантах, которые могут иметь разные торговые названия, например: «Мой ING» или другие. Отдельные версии Системы с разными названиями могут отличаться по своим техническим требованиям;

35) **Телефон авторизации –** номер мобильного телефона пользователя, предназначенный для получения кодов авторизации или выполнения услуг, предусмотренных Договором или настоящими Положениями и условиями. Этот телефон также может использоваться для получения информации или

уведомлений от Банка. Они могут касаться, в частности, безопасности сделки или изменений в Положениях и условиях или других договорных условиях. Номер телефона авторизации указывается Пользователем при подаче заявки на доступ к Системе, заключении Договора или назначении пароля к Системе. Пользователь может изменить номер телефона для авторизации в порядке, установленном Банком;

36) **платежная операция/транзакция –** платеж, перевод или снятие средств, инициированный плательщиком или получателем, который изменяет баланс средств на счете;
37) **бесконтактная транзакция –** вид транзакции, которая осуществляется с использованием бесконтактной технологии на терминале продавца (терминале торговой точки) или банкомате, оснащенном бесконтактным считывающим устройством;
38) **Договор** – заключенный между пользователем и Банком на *Договор об использовании электронных банковских систем* для владельца Счета для беженца, предметом которого является предоставление услуги Системы Интернет-банкинга. Таким договором является *Договор об использовании электронных банковских систем* для владельцев Счета для беженца. Во всех случаях, когда в других документах, включая договоры или дополнения, делается ссылка на *Договор об использовании электронных банковских систем для владельца Счета для беженца, то* под этим подразумевается Договор;
39) **уникальный идентификатор –** комбинация букв, цифр или символов, установленная Банком, которая предоставляется плательщиком/получателем для однозначной идентификации другого плательщика/получателя, участвующего в платежной операции, или его счета. В Положениях и условиях описан уникальный идентификатор для каждого типа транзакции. Если Договором или Положениями и условиями не предусмотрено иное, уникальным идентификатором является номер банковского счета получателя платежа или номер мобильного телефона. Для того чтобы номер мобильного телефона получателя платежа или лица, уполномоченного действовать от его имени, стал уникальным идентификатором, он должен быть ранее связан с единым номером банковского счета получателя платежа или связан с получателем платежа таким образом, который позволяет однозначно идентифицировать этого получателя платежа. Положения и условия этой увязки описаны в Положениях и условиях;
40) **Закон «О платежных услугах», закон –** закон от 19 августа 2011 года «О платежных услугах»;
41) **Аутентификация –** процедура, позволяющая Банку проверить личность пользователя или обоснованность использования данного платежного инструмента, включая его индивидуальные учетные данные. В Положениях и условиях указано, какие данные или информация должны быть предоставлены для подтверждения личности;
42) **мобильное устройство –** многофункциональное портативное устройство с доступом в Интернет, объединяющее функции компьютера и/или мобильного телефона. Перечень операционных систем мобильных устройств, предназначенных для использования с мобильным приложением, указан в § 28 абз. 3 Положений и условий, в Сообщении и на домашней странице Банка;
43) **пользователь –** лицо, являющееся стороной Договора;
44) **Перечень –** перечень мероприятий, проводимых в отделениях Банка и на линии доверия Банка, содержащий информацию об объеме услуг, предоставляемых в данном банковском отделении. Перечень размещен на доске объявлений в отделениях Банка и на веб-сайте Банка и предназначен только для информационных целей;
45) **платежное поручение –** заявление о намерениях плательщика или получателя платежа, адресованное Банку, содержащее указание выполнить платежную операцию.

3. Во всех случаях, когда в Договоре упоминается филиал/отделение Банка в отношении определенной деятельности, под этим понимается отделение Банка, в котором осуществляется данная деятельность. Информация о том, в каком отделении Банка осуществляется деятельность, содержится в Перечне. Перечень размещен на доске объявлений в отделениях банка и на веб-сайте банка.
4. Если в Положениях и условиях упоминается отделение банка в связи с определенным видом деятельности, то информация о том, в каком отделении банка осуществляется этот вид деятельности, содержится в Перечне. Перечень размещен на доске объявлений в отделениях банка и на веб-сайте банка.

§ 2

3. Положения и условия устанавливают условия, на которых Банк предоставляет услуги системы Интернет-банкинга владельцам Счета для беженца.
4. Предметом исполнения являются описанные в Положениях и условиях услуги Системы Интернет-банкинга, которые позволяют Банку осуществлять финансовые услуги посредством Системы.
5. С помощью Системы пользователь имеет доступ только к тем услугам, включая учетные записи, на которые он имеет право. Под уполномоченным лицом понимается лицо, уполномоченное на подачу конкретного распоряжения в соответствии с отдельным соглашением.
6. Если определенные финансовые услуги, доступные в Системе, связаны с риском в силу их специфики или характера деятельности, или вознаграждения, зависящего от движения цен на финансовом рынке, описание этого риска содержится в договорах или положениях и условиях (общих условиях договоров), касающихся данной услуги. Риски, связанные с услугами системы Интернет-банкинга, могут заключаться в нарушении правил безопасности, описанных в Положениях и условиях, в частности, правил безопасного использования системы, описанных в главе 16, или в риске предоставления устройств или приложений в распоряжение неуполномоченных лиц.
7. Система онлайн-банкинга доступна 24 часа в сутки, 7 дней в неделю. Соответствующим временем для исполнения платежных распоряжений и других распоряжений, поданных через Систему, является центральное европейское время (CET) или центральное европейское летнее время в период его введения до его отмены.
8. Предложение заключить Договор, содержание которого включает в себя Положения и условия, не является обязательным, если такой характер прямо не предусмотрен в предложении Банка.
9. Существует Фонд банковских гарантий, который действует в соответствии с правилами, изложенными в Законе об этом фонде. Информационный лист, относящийся к данному фонду, предоставляется Банком владельцу счета в соответствии с договором об отдельном счете. Отправка информационного листа и подтверждение его получения пользователем, являющимся владельцем счета, может осуществляться Системой.
10. Языком, используемым в отношениях Банка со своими клиентами, в том числе когда Банк действует от имени другого лица, как посредник, агент или поверенный, является польский язык.
11. Применимым правом, регулирующим отношения Банка с клиентом до заключения Договора, а также регулирующим правом для заключения и исполнения Договора является польское право (право Республики Польша).
12. Если пользователь, являющийся стороной Договора, является также стороной договора о конкретном банковском счете или стороной других договоров, заключенных с Банком или через Банк, и доступ к этим счетам, услугам или продуктам предоставляется через систему Интернет-банкинга, любые вопросы, не урегулированные в Положениях и условиях регулируют положения заключенных клиентом договоров, включая Положения и условия
13. Пользователь с помощью Системы может, насколько это разрешено законом, осуществлять следующее: идентификацию и аутентификацию в электронной платформе услуг государственного управления, авторизацию, связанную с использованием доверенного профиля, и подтверждение доверенного профиля.
14. Использование названия «Положения и условия предоставления услуг Системы Интернет-банкинга ING Bank Śląski SA» в других нормативных актах, относящихся к продуктам и услугам Банка, означает настоящие Положения и условия.
15. Объявление не является неотъемлемой частью Положений и условий и предназначено исключительно для информационных целей. Изменение содержания Объявления не влечет за собой изменение Положений и условий и не требует прекращения действия Положений и условий.
16. Банк приводит полный текст Объявления:

    1) в банковских учреждениях – на доске объявлений,

2) на веб-сайте Банка.

17. Изменение содержания Перечня не влечет за собой внесение поправок в Положения и условия и не требует прекращения действия Перечня. С текущим содержанием Перечня можно ознакомиться на доске объявлений в отделениях Банка и на веб-сайте Банка.

2. Заключение договора

§ 3

1. Договор заключается на определенный срок.

2. Договор может быть заключен в банковском отделении, осуществляющем данную деятельность, однако Банк оставляет за собой право исключить возможность заключения Договоров в отдельных банковских отделениях,

3. Договор может быть заключен клиентом, который является физическим лицом, обладающим полной дееспособностью,

4. Банк не предоставляет доступ к системе Интернет-банкинга частично недееспособным лицам или полностью недееспособным лицам.

5. Банк, если того требует закон, перед предоставлением пользователю некоторых функций/услуг, указанных в Сообщении, проверяет личность пользователя по документу, удостоверяющему личность, предъявленному пользователем во время его физического присутствия в отделении банка. Данное положение не применяется, если такая проверка была проведена в процессе заключения Договора.

2. Предоставление доступа к Системе

§ 4

1. В момент подачи заявки на доступ к Системе или, самое позднее, после заключения Договора, Банк предоставляет каждому пользователю логин и одноразовый код активации или код авторизации.

2. Для того чтобы воспользоваться системой Интернет-банкинга, Пользователь должен сначала активировать ее. Активация Системы означает назначение самостоятельно определенного пароля, с помощью которого Пользователь будет входить в Систему.

3. Для присвоения пароля к Системе необходимо иметь код авторизации, полученный в виде текстового сообщения, отправленного Банком на номер телефона, указанный пользователем для авторизации, или одноразового кода активации, предоставляемого в отделении банка, осуществляющем данную операцию, или по почте на указанный пользователем адрес корреспонденции. Код авторизации и одноразовый код активации могут быть переданы в другой форме, согласованной между Банком и пользователем.

4. Время действия кода авторизации может быть ограничено по соображениям безопасности системы. Стандартное время действия ограничено продолжительностью сессии, то есть временем соединения пользователя с Банком. Одноразовый код активации действует в течение 30 дней с момента заказа пользователем.

5. Если пользователь получил одноразовый код активации по почте, он обязан позвонить по телефону доверия, чтобы подтвердить его доставку. Если пользователь не подтвердит доставку одноразового кода активации по телефону, он не сможет назначить пароль и пользоваться Системой.

6. Если упаковка с одноразовым кодом активации повреждена или одноразовый код активации неразборчив, пользователь должен немедленно подать претензию.

§ 5

1. Банк информирует пользователя о способе предоставления логина при заключении Договора или при подаче заявки на доступ к Системе Интернет-банкинга.

§ 6

1. Для присвоения пароля к Системе Пользователю необходимо заполнить соответствующую анкету, которую можно найти на веб-сайте Банка. Пользователю также может быть предложено установить пароль к Системе при подаче заявки на доступ к Системе Интернет-банкинга.
2. В целях обеспечения информационной безопасности Системы или безопасности размещенных средств Банк может поставить подачу заявок в зависимость от предоставления пользователем определенных личных данных или информации, относящейся к данной услуге.
3. Если пользователь не использовал одноразовый код активации/код авторизации в течение срока его действия, он должен запросить его переназначение у Банка.

3. Аутентификация пользователя

§ 7

1. Пользователь входит в систему Интернет-банкинга лично, используя только свои данные, которые его аутентифицируют (например, логин, который присвоил ему Банк).
2. Аутентификация пользователя требуется как при входе в Систему, так и при инициировании электронного платежного поручения. С учетом абз. 3, 4 и 5 аутентификация пользователя при входе в систему Интернет-банкинга включает следующие шаги:
   1) предоставление действительного логина,
   2) предоставление пароля в замаскированном виде, что означает предоставление пользователем произвольно указанных Системой символов, составляющих пароль,
   3) и, если это требуется по закону или по соображениям безопасности, предоставление дополнительно соответствующего кода авторизации, или подтверждение в мобильном приложении, если у пользователя есть мобильное приложение, или использовать ключ безопасности, если у пользователя есть активированный ключ в списке ключей безопасности

   Если при входе пользователя в Систему Банк требует предоставления всей информации, указанной в пунктах 1) – 3), это называется строгой аутентификацией. Банк использует строгую аутентификацию, когда это требуется по закону.
3. Аутентификация пользователя при входе в мобильное приложение требует выполнения следующих действий на доверенном мобильном устройстве:
   1) предоставление правильного логина – при первом и последующих входах в систему,
   2) введение пароля в замаскированном виде при первом входе в систему, и вводить PIN-код при последующих входах,
   3) если мобильное приложение установлено на мобильном устройстве, оснащенном считывателем биометрических признаков, последующие входы в систему могут осуществляться с помощью:
      a) биометрического идентификатора, если пользователь выбрал этот метод аутентификации,
      b) и, если это требуется по закону или по соображениям безопасности, дополнительно может потребоваться соответствующий код авторизации, не являющийся биометрическим идентификатором (например, SMS-код или PIN-код).
   4) дополнительно, если это требуется по закону или по соображениям безопасности, использовать ключ безопасности, если у пользователя есть активированный ключ в списке ключей безопасности.

   Аутентификация называется строгой аутентификацией, если при входе в мобильное приложение Банк требует от пользователя наличия доверенного мобильного устройства и, кроме того, предоставления всей информации, указанной в пунктах 1) и 2) или информации, указанной в пункте 3). В целях предотвращения несанкционированного входа в систему, Банк имеет право вводить дополнительные средства или методы аутентификации пользователя при входе в Систему и мобильное приложение. Банк может ввести дополнительные средства аутентификации, если это вытекает из положений закона.

4. Аутентификация пользователя с помощью ключа безопасности требует от пользователя:
   1) регистрации ключа безопасности в системе Интернет-банкинга,
   2) активация ключа безопасности в отделении банка, по телефону инфолинии банка или в системе Интернет-банкинга, если банк предоставляет такую возможность, а также выражения согласия на такой метод аутентификации.
5. В соответствии с абз. 7, для выбора метода аутентификации с использованием биометрического идентификатора пользователь должен сначала:
   1) активировать или настроить функцию считывания биометрических характеристик на мобильном устройстве в соответствии с рекомендациями производителя устройства или установленного на нем программного обеспечения,
   2) ввести в память этого устройства одну собственную биометрическую характеристику, которая станет основой для создания биометрического идентификатора пользователя,
   3) выразить согласие на метод аутентификации на основе биометрического идентификатора.
6. Если Банк считает, что техническое или технологическое решение, примененное производителем мобильного устройства для использования считывателя биометрических признаков, представляет риск для ИТ-безопасности Банка или его клиентов, Банк оставляет за собой право отказать в аутентификации пользователя на основе биометрического идентификатора. В этом случае аутентификация пользователя осуществляется в соответствии с принципами, описанными в абз. 3 пункт 1) и пункт 2).
7. Если пользователь использует доверенное мобильное устройство, Банк исходит из того, что любое распоряжение, данное с помощью такого устройства, было дано пользователем при выполнении упрощенной операции аутентификации. В связи с вышеизложенным, пользователь обязан проявлять особую, повышенную осторожность при хранении такого устройства и не предоставлять его в распоряжение третьих лиц сразу же после добавления устройства в перечень. Перечень типов распоряжений, выполняемых Банком на основании аутентификации пользователя, осуществляемой путем ассоциирования пользователя с добавленным им в перечень мобильным устройством, содержится в Объявлении.
8. Надлежащая аутентификация пользователя, выполненная в соответствии с абз. 2 и 3, должна позволить пользователю получить доступ к информации о счетах или других услугах, предоставляемых через Систему, и давать распоряжения в отношении этих счетов и этих продуктов или услуг.
9. Неправильная аутентификация пользователя при входе в Систему, заключающаяся во введении неверного пароля пять раз подряд, приводит к автоматической блокировке доступа к Системе. Счетчик неправильных попыток входа в систему сбрасывается после правильного входа.
10. Неправильная аутентификация пользователя при входе в Мобильное приложение путем ввода неправильного PIN-кода три раза подряд приводит к блокировке доступа пользователя к Системе. Счетчик попыток ввода PIN-кода сбрасывается после правильного входа в систему. Повторное присвоение PIN-кода возможно после правильного ввода пароля в замаскированном виде.
11. Если пользователь использовал считыватель биометрических признаков при входе в мобильное приложение и пользователь не был аутентифицирован на основе биометрического идентификатора, вход в мобильное приложение будет возможен после ввода действительного PIN-кода или другого кода авторизации.

4. Подача волеизъявлений и заявлений о полной осведомленности в электронном виде

§ 8

1. На основании заключенного Договора пользователь и Банк могут посредством Системы Интернет-банкинга в электронной форме делать волеизъявления или заявления о своей полной осведомленности, связанные с осуществлением:
   1) банковской деятельности, или
   2) иной деятельности в соответствии с Уставом Банка.

   Такие заявления могут быть сделаны с оговоркой, что в связи с постоянным развитием информационных технологий отдельные функциональные возможности, предоставляемые посредством системы Интернет-банкинга, могут изменяться или становиться доступными в разное время. Информация о возможности сделать определенные волеизъявления заявления о своей полной осведомленности, в определенное время описана в Объявлении.
2. Волеизъявления в электронной форме, связанные с осуществлением деятельности, указанной в абз. 1 пункт 1) и пункт 2), считаются такими волеизъявлениями, которые связаны с установлением, осуществлением, изменением, прекращением, расторжением или истечением срока действия правоотношений, касающихся этой деятельности. Таким заявлением является также выдача, изменение или отзыв доверенности, связанной с осуществлением деятельности, указанной в абз.1, пункт 1) и пункт 2).
3. В той мере, в какой волеизъявления, сделанные в электронной форме, отвечают требованиям закона для признания их сделанными в письменной форме, они считаются сделанными в письменной форме, даже если такое требование предусмотрено под страхом недействительности. В случае распоряжений, в том числе требующих письменной формы, подпись может быть выполнена в электронной форме, если она отвечает требованиям электронной формы, эквивалентной письменной форме, согласно соответствующим положениям закона. Такая подпись в электронной форме может быть выполнена в виде квалифицированной электронной подписи, усовершенствованной электронной подписи или иной электронной подписи в смысле общепринятого законодательства, в том числе:
   1) путем передачи другой стороне данных, идентифицирующих пользователя или Банк, или
   2) любым другим способом, разрешенным законом.
4. Если положения закона позволяют признать тот или иной способ авторизации распоряжения в качестве подписи в электронной форме, пользователь может поставить такую подпись путем авторизации. Если Банк ставит подпись в электронной форме, отправляя идентификационные данные другой стороне, то подпись, отправленная через Систему, содержит идентификационные данные лица, представляющего Банк. Банк и пользователь посредством волеизъявлений, составленных с использованием Системы Интернет-банкинга, могут в приложении к договору, заключенному в электронной форме, ввести иной способ проставления подписи в электронной форме, если в соответствии с правовыми нормами считается, что проставление подписи в данной форме удовлетворяет требованиям письменной формы.
5. Банк и пользователь могут совершать действия, заключать договоры/приложения к договорам или делать заявления, требующие письменной формы, в электронной форме, эквивалентной письменной форме. В той мере, в какой это разрешено законом, Банк и пользователь могут использовать Систему для составления других деклараций, требующих письменной формы, в электронной форме, эквивалентной письменной форме.
6. Если из информации, заявления или документа, имеющегося в Системе, следует, что заявление Банка или волеизъявление или заявление о своей полной осведомленности пользователя относится к более чем одному распоряжению или более чем одному заявлению или документу, считается, что одна электронная подпись относится ко всем распоряжениям или всем переданным заявлениям или документам.
7. Банк направляет пользователю корреспонденцию, в том числе любые волеизъявления или заявления о своей полной осведомленности, образцы документов, а также заключенные пользователем договоры

вместе с положениями и условиями и другие документы посредством системы Интернет-банкинга, если общепринятыми законами не предусмотрено иное. Корреспонденция, включая декларации о намерениях или знании, отправляемая Банком, может иметь квалифицированную электронную печать, усовершенствованную электронную печать или другую электронную печать, предписанную общепринятым законодательством

8. Банк может разрешить пользователю доставлять корреспонденцию в Банк в электронном виде через Систему. В связи с развитием информационных технологий конкретные виды заявлений (корреспонденции), предоставляемых через Систему, могут меняться или предоставляться в разное время. Информация о возможности подачи определенных видов заявлений (корреспонденции) в определенное время описана в Сообщении.
9. Банк направляет пользователю в электронном виде, в том числе через Систему, объявления, подтверждающие факт заключения определенного договора или принятия распоряжения к исполнению.

5. Электронная доставка корреспонденции

§ 9

1. В рамках системы Интернет-банкинга Банк предоставляет пользователю доступ:
   1) к ящику «сообщения», который используется для связи Банка с пользователем,
   2) к Системе доставки электронной корреспонденции, в которой Банк будет размещать изменения в договорных правилах, которые по закону должны быть переданы на долговечном носителе. Использование названия «Электронная система доставки корреспонденции» в других нормативных документах, относящихся к продуктам и услугам Банка, означает именно эту услугу. Пользователям Электронной системы доставки корреспонденции Банк также будет предоставлять выписку по счету, выписку по операциям с кредитной картой и другие документы, которые по закону должны быть доставлены на долговечном носителе.
2. Банк не несет ответственности за последствия непрочтения документов/сообщений/корреспонденции, отправленных через систему Интернет-банкинга. Пользователь обязан читать сообщения, отправляемые ему Банком через Систему. Вышеизложенное не ограничивает право Банка направить корреспонденцию пользователю по почте на адрес, указанный пользователем, или вручить корреспонденцию пользователю лично в отделении банка, осуществляющем данную деятельность.
3. Начиная с даты предоставления Банком доступа к Электронной системе доставки корреспонденции, изменения в договорных положениях, которые по закону должны направляться на долговечном носителе, будут доводиться Банком до пользователей, являющихся сторонами Договора, в Электронной системе доставки корреспонденции. Это позволяет Клиенту хранить адресованную ему информацию таким образом, который допускает доступ к ней в течение периода, соответствующего цели подготовки этой информации, и позволяет восстановить сохраненную информацию в неизменном виде. Это пространство является неотъемлемой частью Системы и может фигурировать под другим торговым названием. Доступ к нему не требует отдельного договора.
4. Пользователь будет иметь доступ к Электронной системе доставки корреспонденции до прекращения действия Договора. До расторжения Договора пользователь может распечатать или сохранить на другом долговечном носителе документы, которые Банк вручил ему в Электронной системе доставки корреспонденции.
5. По окончании срока действия Договора Банк предоставляет пользователю доступ к содержимому Электронной системы доставки корреспонденции через Архив документов (далее: Архив), в той мере, в какой Банк предоставляет такую возможность, или предоставит такому пользователю содержимое этой системы на другом постоянном носителе информации.
6. Для входа в Архив пользователю необходимо предоставить Банку свой адрес электронной почты и номер телефона для авторизации. Эти данные необходимы для входа клиента в Архив.

7. При использовании Архива пользователь должен соблюдать правила безопасности, предусмотренные Положениями и условиями. Если пользователь подозревает, что неуполномоченное лицо получило доступ к его/ее Архиву, он обязан немедленно заблокировать доступ к своему Архиву или изменить данные, необходимые для использования Архива (e-mail, номер телефона для авторизации).
8. Банк имеет право заблокировать доступ к Архиву в соответствии с основаниями для блокировки Системы. Пользователь также может сам заблокировать доступ к Архиву.
9. Дать команду на разблокировку Архива или изменить данные для входа в Архив пользователь может только в отделении банка, осуществляющем данную деятельность.
10. Подробности, связанные с использованием Архива пользователем, можно найти в Объявлении.

6. Представление распоряжений, их авторизация и исполнение

§ 10

1. Банк выполняет указания только того пользователя, которому он присвоил логин.
2. Пользователь не вправе давать через Систему указания, связанные с участием в азартных играх, объектом которых является предоставление Банком платежных услуг, если только игра не проводится в соответствии с Законом «Об азартных играх». Банк имеет право отказаться от выполнения таких распоряжений.
3. Подать распоряжение в мобильном приложении можно будет до тех пор, пока мобильное устройство находится в списке доверенных мобильных устройств на момент подачи распоряжения.
4. Банк имеет право устанавливать лимиты на сумму и количество платежных операций, осуществляемых на основании платежных распоряжений, которые выполняются с помощью системы Интернет-банкинга.
5. В случаях, предусмотренных законом, Банк обеспечивает выполнение распоряжений, в том числе платежных поручений, при условии строгой аутентификации пользователя. Если банк требует, чтобы строгая аутентификация пользователя происходила через мобильное приложение, пользователь обязан иметь доверенное мобильное устройство при выполнении того или иного действия.

§ 11

1. Банк осуществляет платежные операции после их авторизации пользователем. Авторизация платежного поручения пользователем означает его согласие на осуществление платежной операции. Согласие на проведение платежной операции может быть также дано пользователем через получателя, поставщика получателя или поставщика, предоставляющего услугу по инициированию платежной операции.
2. Авторизация распоряжений, в том числе платежных поручений, поданных пользователем через систему Интернет-банкинга, включает:
   1) выбор кнопки акцепта – когда Банк считает, что данное распоряжение может быть авторизовано таким образом из-за правил безопасности, или
   2) выбор кнопки акцепта в мобильном приложении (мобильная авторизация) – когда Банк считает, что соответствующее распоряжение должно быть авторизовано в мобильном приложении. Этот метод авторизации требует одновременного физического владения пользователем доверенным мобильным устройством, на котором установлено и активировано мобильное приложение, или
   3) ввод правильного кода или кодов авторизации, включая биометрический идентификатор, и выбор кнопки приема – когда Банк обнаруживает, что данное платежное поручение в силу положений закона или правил безопасности требует авторизации путем ввода кода или кодов авторизации, или
   4) ввод правильного кода или кодов авторизации, включая биометрический идентификатор и приближение мобильного устройства к терминалу или
   5) использование ключа безопасности, если пользователь имеет активированный ключ в списке ключей безопасности и если Банк решит, что данное распоряжение с учетом требований безопасности может быть авторизовано в таком порядке, или

6) использование физической платежной карты с возможностью бесконтактной оплаты путем поднесения ее к мобильному устройству с установленным мобильным приложением и включенной функцией NFC.

3. Для аутентификации распоряжения с помощью биометрического идентификатора сначала пользователь должен:

1) активировать или настроить функции считывания биометрических характеристик на мобильном устройстве в соответствии с рекомендациями производителя устройства или установленного на нем программного обеспечения,

2) ввести в память этого устройства конкретную биометрическую характеристику пользователя, на основе которой будет создан его биометрический идентификатор, и согласовать дополнительный метод аутентификации и метод авторизации распоряжений с помощью биометрического идентификатора.

4. В целях безопасности Банк оставляет за собой право отказать в авторизации распоряжения, сделанного на основе биометрического идентификатора. Причиной этого может быть то, что Банк считает, что техническое или технологическое решение, используемое производителем мобильного устройства для использования считывателя биометрических признаков, представляет собой риск, угрожающий информационной безопасности Банка или его клиентов. В этом случае авторизация распоряжений осуществляется в соответствии с принципами, описанными в абз. 2, исключая возможность использования для этой цели биометрического идентификатора.

5. Каждое указание пользователя, которое должно быть выполнено Системой и которое повлечет за собой изменение остатка денежных средств на счетах, или будет являться заявкой Банка на заключение нового договора или выполнение услуги, или будет связано с такой заявкой, требует авторизации пользователя в соответствии с абз. 2.

6. Авторизация распоряжений с помощью ключа безопасности требует от пользователя:
1) регистрации ключа безопасности в системе Интернет-банкинга,
2) активация ключа безопасности в отделении банка, по телефону инфолинии банка или в системе Интернет-банкинга, когда банк предоставляет такую возможность, и дано согласие на такой способ авторизации распоряжения.

7. Применяя принципы безопасности, Банк проверяет, авторизован ли пользователь при подаче распоряжений путем:

1) проверки правильности данных, предоставленных пользователем при входе в Систему, как указано в § 7 абз. 2 и 3,

2) проверки, выбрал ли пользователь кнопку принятия распоряжения, которая была распознана Банком как не требующая авторизации путем предоставления кода авторизации,

3) проверка правильности кода или кодов авторизации, предоставленных Банком и переданных пользователем, включая биометрический идентификатор, или проверка использования ключа безопасности, если пользователь имеет активированный ключ в списке ключей безопасности.

Если результат вышеуказанной проверки отрицательный, Банк считает, что распоряжение не авторизовано пользователем, и отказывается его выполнять.

8. Банк предоставляет пользователю коды авторизации, которые являются SMS-кодами, в SMS-сообщении на телефонный номер, ранее указанный пользователем для авторизации.

9. Срок действия предоставленного Банком кода авторизации может быть ограничен по соображениям безопасности Системы. Стандартное время действия ограничено продолжительностью сессии, т.е. временем соединения пользователя с Банком через Систему. Код авторизации генерируется для поданного распоряжения и может быть использован только для авторизации этого распоряжения. Вместе с кодом авторизации пользователь получает информацию о деталях распоряжения.

10. В случае пятикратного неверного указания переданного Банком кода авторизации для утверждения данного распоряжения, доступ к системе Интернет-банкинга блокируется. В случае трехкратного

введения неправильного PIN-кода для подтверждения распоряжения в мобильном приложении, Банк может заблокировать доступ к системе Интернет-банкинга.

11. Распоряжение о разблокировании доступа к Системе может быть дано в отделении банка, выполняющем данное действие, через веб-сайт Банка или в Системе, если Банк допускает такую функциональность. В каждом случае для разблокировки пользователь должен заново ввести пароль или PIN-код для мобильного приложения.

12. В целях безопасности Банк оставляет за собой право в отношении каждого распоряжения запрашивать дополнительную авторизацию, например, с помощью кодов авторизации, ключей безопасности, если у пользователя есть активированный ключ в списке ключей безопасности.

§ 12

1. Распоряжение, данное пользователем в системе Интернет-банкинга, является безотзывным и окончательным волеизъявлением пользователя, с учетом абз. 5.

2. Поручения, переданные через Систему, могут относиться только к счетам и банковским продуктам или услугам, доступным пользователю через Систему.

3. Информация о порядке исполнения отдельных распоряжений, поданных с использованием системы Интернет-банкинга, содержится в приложении 1 и на домашней странице Банка в главе, посвященной системе.

4. Моментом получения Банком платежного поручения, поданного через систему Интернет-банкинга

1) в рабочий день или в субботу до времени отключения, указанного в приложении 1, с учетом пункта 3), считается момент авторизации платежного поручения, как указано в § 11 абз. 2,

2) в рабочий день или в субботу после времени отключения, указанного в приложении 1, или в праздничный день, с учетом пункта 3), считается первый рабочий день, следующий за днем подачи платежного поручения, за исключением платежных распоряжений, указанных в приложении 1, для которых не установлено время отключения приема платежных распоряжений, для которых моментом получения платежного поручения считается момент, указанный в пункте 1),

3) с отсроченной датой платежа (перевод, исполнение которого начинается в день, отличный от того, в который размещено платежное поручение):

a) является дата, указанная пользователем для списания средств со счета;

b) Если день, указанный пользователем для списания средств со своего счета, не является рабочим днем (за исключением субботы), платежное поручение считается полученным в первый рабочий день, следующий за днем, указанным пользователем для списания средств со своего счета, с учетом распоряжений, указанных в пункте c);

c) Если день, указанный пользователем для списания средств со счета, не является рабочим днем (за исключением субботы), то в случае платежных распоряжений, указанных в приложении 1, для которых не установлено время приема платежных распоряжений, моментом поступления таких платежных поручений в Банк считается день, указанный пользователем для списания средств со счета;

d) Если день, указанный пользователем для списания средств со счета, выпадает на субботу, платежное поручение считается полученным в этот день, с учетом распоряжений, указанных в пункте e);

e) Если день, указанный пользователем для списания средств со счета, выпадает на субботу, то для платежных распоряжений, указанных в приложении 1, для которых установлено время окончания приема платежных распоряжений, временем получения Банком таких платежных распоряжений считается первый рабочий день, следующий за днем, указанным пользователем для списания средств со счета.

5. С учетом абз. 6 пользователь не может отозвать платежное поручение с момента его получения Банком, если иное не предусмотрено другими нормативными актами или отдельно заключенными договорами.

6. В случае исходящего платежного поручения, указанного в приложении 1, пользователь может отозвать его до даты и времени, указанных в приложении 1.
7. Если платежная операция инициируется поставщиком услуг, предоставляющим услугу инициирования платежной операции, или получателем платежа или через него, за исключением отложенного платежного поручения, упомянутого в абз. 4 пункт 3), плательщик не может отозвать платежное поручение после предоставления поставщику услуг, инициирующему платежную операцию, своего согласия на выполнение платежной операции или после предоставления своего согласия получателю платежа на совершение платежной операции.

§ 13

1. Банк выполняет распоряжения, в том числе платежные поручения, поданные через систему Интернет-банкинга, на принципах, предусмотренных Положениями и условиями, а в вопросах, не урегулированных настоящими Положениями и условиями, на принципах, предусмотренных в отдельных обязательных для клиента положениях и условиях, касающихся соответствующих счетов или других услуг, к которым относится данное распоряжение.
2. В случае расторжения Договора отложенное платежное поручение, ранее поданное Системой, будет исполнено в соответствии с указанием пользователя.
3. В соответствии с абз. 5 Банк отказывается выполнять распоряжение, в том числе платежное поручение, по причинам, указанным в договоре или Положениях и условиях, обязательных для пользователя и относящихся к соответствующему счету, а также распоряжение, которое является:
   1) неполным или неправильным из-за неверного уникального идентификатора или другой неверной информации, необходимой для выполнения распоряжения,
   2) противоречит другому уже сделанному распоряжению,
   3) не может быть исполнено из-за недостаточного количества средств на счете, необходимого для его исполнения,
   4) несанкционированным в порядке, описанном в Положениях и условиях,
   5) по иным причинам, прямо предусмотренным Положениями и условиями, Договором или общеприменимым законодательством.

   Это относится ко всем платежным распоряжениям, в том числе инициированным получателем платежа или через него.
4. Пользователь должен быть незамедлительно уведомлен о любом отказе Системы выполнить распоряжение. По возможности, Пользователь также получит информацию о причинах отказа или процедуре исправления ошибок, вызвавших отказ, если такое уведомление не является недопустимым по отдельным нормативным актам.
5. В случае, если лицо, подающее распоряжение в Системе Интернет-банкинга, не обновляет в Банке документ, удостоверяющий личность, Банк имеет право отказать в выполнении платежного поручения.
6. Банк осуществляет платежные операции на одинаковой основе независимо от того, подано ли платежное поручение пользователем непосредственно в Банк или инициировано поставщиком, предоставляющим услугу инициирования платежной операции, если положениями Правил не предусмотрено иное.

§ 14

Информация, предусмотренная законом, должна периодически, не реже одного раза в месяц, бесплатно предоставляться через Систему, если иное не предусмотрено отдельным обязательным для пользователя постановлением или Положениями и условиями.

§ 15

1. Когда пользователь подает распоряжение, являющееся платежным поручением, в отделении банка, осуществляющем данную деятельность, или через телефон доверия, пользователь может, если Банк предоставляет такую возможность, авторизовать такое распоряжение, сообщив в этом отделении или

через инфолайн код авторизации, полученный посредством SMS-сообщения, отправленного Банком на телефонный номер пользователя для авторизации.

2. Если пользователь подает распоряжение, не являющееся платежным поручением, в отделении банка, осуществляющем данную деятельность, или через телефон доверия, пользователь может, если Банк предоставляет такую возможность, подать такое распоряжение, за исключением распоряжений, для которых Положения и условия предусматривают подачу только в письменном виде или через систему Интернет-банкинга, сообщив в отделении или через Информационный центр код авторизации, полученный посредством SMS-сообщения, отправленного Банком на телефонный номер пользователя для авторизации. Перечень распоряжений указан в Объявлении.
3. Если банк предоставляет такую возможность, пользователь может подать распоряжение, которое является платежным поручением, или распоряжение, которое не является платежным поручением, и авторизовать его, поставив подпись на электронном устройстве в отделении банка, осуществляющем это действие в соответствии со статьей 7 абз. 1 Закона «О банках», после предоставления банку своих идентификационных данных и подтверждения личности лица, делающего заявление, сотрудником банка. Документы, на основании которых Банк подтверждает личность, указаны в Объявлении для владельцев счетов, изложенном в Положениях и условиях предоставления услуг ING Bank Śląski S.A. в рамках ведения Счета для беженца. Электронное устройство обеспечивает запись и целостность содержания заявления, поставленной подписи, а также даты и времени подачи заявления. Если волеизъявление клиента связано с установлением, исполнением, изменением, прекращением, расторжением или истечением срока действия правоотношений, связывающих его с Банком, и требует представления Банком волеизъявления, Банк представляет подпись в электронной форме, помещая в ее содержание данные, идентифицирующие его представителя, т.е. имя и фамилию и идентификационный номер сотрудника.

7. Услуги по поддержке финансового управления

§ 16

1. В рамках Системы Банк предоставляет услуги по поддержке финансового управления (далее: финансовое управление). Эти услуги носят консультативный и совещательный характер и связаны, в частности, с платежами.
2. Для предоставления этих услуг Банк предоставляет функциональные возможности Системы, которые учитывают индивидуальные потребности пользователя. Для того чтобы Банк мог осуществлять финансовое управление, необходимо классифицировать финансовую информацию и профилирование персональных данных, касающихся пользователя, в соответствии с Постановлением (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 г. – Общее положение о защите данных. Профилирование может осуществляться только в той мере, в какой это необходимо для финансового управления. Осуществляя финансовое управление, Банк не принимает решения по финансовым вопросам за клиента.
3. Финансовое управление не включает консультационные услуги, управление портфелем, подготовку инвестиций, финансовый анализ и другие рекомендации в смысле статьи 69 абз. 2 и абз. 4 Закона «О торговле финансовыми инструментами», которые могут предоставляться Банком на основании других договоров/регламентов, даже если они предоставляются дистанционно Системой.
4. Управление финансами осуществляется в форме:

   1) информации или уведомления о:

   a) финансовой терминологии и знаниях в этих областях,

   b) будущих платежах, в том числе периодически производимых клиентом, а также будущих событиях или сроках,

   c) возможных будущих платежах клиента, включая периодические платежи,

   2) представления финансовой ситуации пользователя с указанием:

a) типа проводимых им операций или принадлежности операций к определенной группе или типу операций,

b) вида или категории деловых поступлений, расходов или контрагентов,

5. Информация, презентации и консультации, упомянутые в абз. 4, могут принимать различные графические или текстовые формы.

6. Управление финансами будет осуществляться в соответствии со следующими принципами:

1) Информация о сроках предоставляется в Системе на постоянной основе, а уведомления о будущих сделках/событиях или сроках предоставляются не позднее чем за 48 часов до указанной в Системе сделки/события или срока,

2) презентации финансового положения готовятся на ежемесячной или ежегодной основе на основе произведенных или ожидаемых платежей. Эти презентации могут также включать информацию, предоставленную пользователем в Системе или другими лицами, уполномоченными пользователем. Система может допускать различные настройки периода данной презентации.

7. Управление финансами является неотъемлемой частью Системы, за исключением того, что в рамках этих услуг отдельные функциональные возможности могут быть активированы пользователем самостоятельно.

§ 17

1. При надлежащем осуществлении финансового управления Банк несет ответственность за доказанные убытки пользователя, с учетом абз. 2.

2. Банк не несет ответственности за цели, обязательства или пределы расходов, установленные пользователем, а также за их реализацию и уровень исполнения.

3. Банк не несет ответственности за решения пользователя по управлению финансами, включая решения, касающиеся приобретения определенных услуг или инвестирования средств. Исключение ответственности не распространяется на ситуации, когда Банк нарушил свою обязанность действовать с должной осмотрительностью или нарушил обязательные положения закона.

4. Банк готовит консультацию в меру своей воли и знаний и с должной осмотрительностью, основываясь на известных Банку фактах, существующих на момент ее предоставления, в частности, на информации, предоставленной пользователем. Банк не проверяет достоверность информации, предоставленной пользователем. Чтобы получить достоверную консультацию, пользователь обязан предоставить правдивую информацию, в частности, о своем финансовом положении.

5. Если в рамках управления финансами определенная функциональность активируется пользователем самостоятельно, Банк – независимо от своих обязательств по информированию в соответствии с законодательством – может предоставить дополнительную информацию о рисках, связанных с услугами. Пользователь обязан ознакомиться с такой информацией и принимать разумные решения относительно инвестирования средств.

6. В связи с постоянным развитием информационных технологий отдельные функциональные возможности, доступные в рамках финансового управления, могут изменяться или запускаться в Системе в разное время. Информацию об их наличии можно найти в Объявлении. Эти функциональные возможности могут иметь различные обозначения и названия.

7. Финансовое управление осуществляется до истечения срока действия или расторжения Договора. После этого момента пользователь не имеет доступа к результатам предоставления услуг по поддержке финансового управления, подготовленным Банком, в частности к информации, презентациям, консультациям и финансовым целям или проектам, которые определил пользователь. До истечения срока действия или расторжения Договора Пользователь может распечатать результаты финансовой консультации или хранить их на электронном носителе – при условии, что Система позволяет подготовить консультацию в виде текстового файла.

8. Электронный сейф в системе Интернет-банкинга

§ 18

1. Электронный сейф (далее: сейф) — это услуга, которая заключается в хранении сохраненных пользователем электронных документов (также называемых: файлы) в специально отведенном месте системы Интернет-банкинга. Это пространство является неотъемлемой частью Системы и может фигурировать под разными торговыми названиями.
2. Банк предоставляет услугу сейфового хранения пользователям, заключившим Договор. Использование данной услуги не требует заключения отдельного договора. В безопасном пространстве пользователь может хранить файлы, загружать или удалять ранее сохраненные им файлы. Пользователь не может редактировать сохраненные файлы или изменять их форматы.
3. Каталог форматов файлов, которые могут быть сохранены в Системе, приведен в Сообщении.
4. Пользователь получает доступ к сейфу в момент входа в Систему. Пользователь может использовать сейф, войдя в Систему.
5. Сейф связан с логином пользователя. Если у пользователя несколько логинов, услуга доступна отдельно для каждого логина. Невозможно использовать один и тот же сейф для нескольких логинов.
6. Информация о доступной вместимости сейфа указана в Системе.
7. Пользователь несет ответственность за содержание сохраненных файлов и их формат. Пользователь может хранить в сейфе только те файлы, на которые он должным образом уполномочен, которые не нарушают действующее законодательство, были созданы или получены в соответствии с законом и не нарушают права третьих лиц, включая личные права, авторские права, права промышленной собственности или коммерческие тайны таких лиц. Пользователь может сохранять только те файлы, которые не содержат электронных вирусов или каких-либо частей опасного программного обеспечения.
8. Банк имеет право отказать пользователю в хранении в сейфе документа, который не соответствует техническим требованиям, угрожает безопасности Банка, электронных систем Банка или других пользователей, или денежных средств, находящихся в Банке. Узнав о нарушении положений § 27 абз. 7, Банк отказывает пользователю в размещении файлов. В случае, если нарушение безопасности или нарушение обязательств, указанных в абз. 7, может привести к серьезным убыткам для Банка или других пользователей, Банк имеет право ввести в действие соответствующее программное обеспечение безопасности и, в случаях срочного риска, изолировать и, если это невозможно, удалить сохраненные файлы.
9. Банк не имеет доступа к файлам и документам, помещенным пользователем в сейф, не проверяет и не верифицирует содержащиеся в них данные и содержание. Банк несет ответственность, предусмотренную Положениями и условиями, с момента сохранения данного файла в сейфе.
10. При хранении файлов, сохраненных пользователем, при должной осмотрительности, Банк не несет ответственности за:
    1) содержание и данные, содержащиеся в файлах и документах, загруженных в Систему,
    2) изменение названия файла, сделанное пользователем,
    3) файлы, извлеченные из сейфа во время дачи распоряжения,
    4) последствия любого нарушения пользователем прав, описанных в абз. 7 или абз. 8,
    5) оставление файла в сейфе по истечении срока действия или расторжении договора о Системе,
    6) убытки и расходы, возникшие в результате любого повреждения файла, его полного повреждения или перехвата файла во время его передачи в Систему, за исключением случаев, когда они возникли в результате работы ИТ-системы Банка,
    7) неспособность Банка определить в момент сохранения файла в Системе наличие в нем вирусных элементов,
    8) задержка в выполнении или невыполнение распоряжений пользователя в пределах сейфа, если это вызвано форс-мажорными обстоятельствами.

11. Банк предоставляет содержимое сейфа уполномоченным законом органам, не анализируя содержащиеся в нем файлы, в порядке, предусмотренном соответствующими положениями Закона «О банках».

12. Банк не несет ответственности за любой ущерб, возникший в результате раскрытия содержимого сейфа лицам или учреждениям, уполномоченным запрашивать такую информацию у Банка.

13. Пользователь теряет доступ к сейфу и хранящимся в нем файлам/документам по истечении срока действия или расторжении Договора. При прекращении работы Системы файлы/документы, хранящиеся в сейфе, автоматически и навсегда удаляются Банком. Банк не хранит копии этих файлов/документов. Перед прекращением/расторжением Договора Банк уведомит пользователя о необходимости загрузить сохраненные файлы. Оповещение может осуществляться любым способом, в том числе с помощью объявления, отображаемого пользователю в Системе.

14. По техническим причинам, в связи с развитием технологий и программного обеспечения, используемого для работы сейфа, или в целях безопасности, Банк имеет право ограничить возможность использования хранения файлов определенных форматов в пространстве сейфа или ограничить функциональность сейфа. В этом случае пользователь будет проинформирован в Системе до того, как будет предпринято определенное действие.

9. Использование платежных услуг, предоставляемых уполномоченными третьими лицами

§ 19

1. Пользователь может, в рамках своих прав, пользоваться платежными услугами третьих лиц, например, предоставляющими доступ к информации о счете или услугами по инициированию платежной операции:

1) услуга доступа к информации о счете – выполняется поставщиком услуги доступа к информации о счете, заключается в отправке Банком – по запросу этого поставщика – информации о счете, хранящемся в Банке;

2) услуга инициирования платежной операции – выполняется поставщиком услуги инициирования платежной операции, заключается в инициировании этим поставщиком, действующим по запросу пользователя, платежного поручения с платежного счета, открытого в Банке, на которое имеет право пользователь.

2. Использование услуги доступа к информации о счете возможно при условии, что обслуживаемый Банком счет является платежным счетом, доступным в режиме онлайн, и пользователь аутентифицирован Банком, в соответствии с требованиями законодательства и положениями Условий.

3. Использование услуги по инициированию платежной операции возможно при условии, что в соответствии с обязательными для пользователя правилами это безналичная электронная операция, связанная с платежным счетом, доступным в Интернете, что она инициируется исключительно в результате распоряжения пользователя, и что, кроме того, пользователь аутентифицирован Банком в соответствии с требованиями законодательства и Положениями и условиями.

4. Банк предоставляет Поставщику услуг по предоставлению информации о счетах информацию о назначенных счетах и связанных с ними операциях, включая историю таких счетов – за исключением того, что период, за который Банк предоставляет историю счетов, может быть ограничен по технологическим причинам.

5. Банк не несет ответственности за надлежащее выполнение услуг, указанных в абз. 1, уполномоченными третьими лицами.

6. Пользователь может дать разрешение в Системе на то, чтобы Банк отвечал на запросы поставщика, выпускающего платежные инструменты на основе платежной карты, о наличии на платежном счете суммы, соответствующей конкретной платежной операции, совершенной на основе этой карты.

7. Платежный счет доступен в режиме онлайн при выполнении всех следующих условий:

1) пользователь является стороной Договора,

2) у пользователя есть активный доступ к системе Интернет-банкинга,

3) соответствующий платежный счет становится доступным Системе после получения Банком соответствующего запроса или запроса от соответствующего провайдера на выполнение действия для предоставления услуги, указанной в абз. 1.

8. Платежный счет не доступен в режиме онлайн, когда Банк получает соответствующее заявление или запрос на действие:

   1) у пользователя нет активной системы Интернет-банкинга, или

   2) когда доступ к Системе заблокирован, или

   3) если пользователь использовал функцию скрытия данной учетной записи в Системе и не отозвал это указание.

9. Банк вправе отказать поставщику доступа к информации о счете или поставщику услуги инициирования платежной операции в доступе к данному платежному счету по объективно обоснованным и надлежащим образом документированным причинам, связанным с несанкционированным или незаконным доступом такого поставщика к платежному счету, включая несанкционированное инициирование платежной операции. В этом случае Банк информирует пользователя через Систему об отказе в доступе к платежному счету и причинах такого отказа. Такая информация по возможности сообщается пользователю до отказа в доступе и, самое позднее, сразу после него, но не позднее рабочего дня, следующего за отказом, за исключением случаев, когда ее сообщение нецелесообразно по объективно оправданным соображениям безопасности или противоречит отдельному законодательству.

10. Ответственность банка

§ 20

1. Банк обязуется:

   1) поддерживать конфиденциальность всех данных аутентификации и авторизации пользователей,

   2) предоставлять пользователю доступ через систему Интернет-банкинга к текущей информации о счетах, на которые он имеет право, таким образом, чтобы можно было осуществлять постоянный мониторинг операций, проводимых по этим счетам.

2. Банк несет ответственность за доказанные убытки пользователя, вызванные неисполнением распоряжения или его неправильным или несвоевременным исполнением, если они не являются результатом обстоятельств, за которые Банк не несет ответственности.

3. Банк несет ответственность за последствия, если таковые возникли, исполнения сделки третьими лицами, после того как было сделано указанное в § 22a абз. 4 и 5 пункт 1) уведомление и Пользователь дал указание заблокировать доступ к Системе, начиная с:

   1) получения распоряжения в Банке – если распоряжение было подано через Систему,

   2) письменного подтверждения Банком факта дачи такого распоряжения – если распоряжение дано в отделении банка, осуществляющем данную деятельность,

   3) получения пользователем устного подтверждения по телефону доверия о блокировке доступа к Системе – если указание было дано по телефону доверия,

   - если только он намеренно не совершил несанкционированную транзакцию.

4. Банк несет ответственность за защиту конфиденциальности данных пользователя, используемых для аутентификации и авторизации с помощью системы Интернет-банкинга, только если пользователь использует эти данные в соответствии с принципами, установленными Положениями и условиями, если только конфиденциальность не была нарушена по вине Банка.

5. Банк не несет ответственности за неисполнение или ненадлежащее исполнение Договора, если причиной неисполнения или ненадлежащего исполнения Договора, включая сделки, являются форс-мажорные обстоятельства.
6. Банк не несет ответственности за невыполнение Договора, если отказ от выполнения обязательств по Договору основан на общеприменимых законах, которые разрешают или обязывают Банк отказаться от выполнения таких обязательств или распоряжений.
7. Банк не несет ответственности за:
   1) неисполненные распоряжения – в случае неверной или неполной информации относительно уникального идентификатора или неспособности плательщика или получателя предоставить информацию, необходимую для исполнения данного распоряжения или операции, в той степени, в которой неисполнение распоряжения является результатом неспособности предоставить информацию, необходимую для ее исполнения,
   2) последствия, возникшие в результате работы телекоммуникационного оборудования пользователя в связи с получением SMS-сообщений, при условии, что задержка в получении сообщения произошла не по вине Банка,
   3) ущерб пользователю, возникший в результате несоблюдения пользователем правил безопасности системы Интернет-банкинга.
8. В отношении пользователей, являющихся стороной договора о платежном счете в смысле Закона, Банк несет ответственность за неисполнение или ненадлежащее исполнение правильно заказанной операции, если не докажет, что счет получателя платежа был зачислен в установленный законом срок или когда:
   1) требования пользователя погашены в результате того, что он не сообщил в течение 13-месячного периода, предусмотренного Положениями и условиями, о несанкционированных, неисполненных или ненадлежащим образом исполненных сделках, или
   2) неисполнение или ненадлежащее исполнение сделки произошло вследствие непреодолимой силы или было обусловлено положениями закона.
9. Если в соответствии с Положениями и условиями Банк несет ответственность перед плательщиком или получателем платежа, являющимся пользователем, – он обязуется возместить плательщику или получателю платежа сумму неисполненной или ненадлежащим образом исполненной операции и, если такой пользователь является владельцем платежного счета с точки зрения закона, восстановить счет до состояния, в котором он находился бы, если бы неисполнение или ненадлежащее исполнение операции не имело места. Вышеуказанное также относится к комиссиям или процентам, взимаемым с пользователя в случае неисполнения или ненадлежащего, в том числе несвоевременного, исполнения платежной операции.
10. В случае неисполненной или ненадлежащим образом исполненной платежной операции, инициированной плательщиком или получателем или через них, Банк по просьбе плательщика или получателя немедленно принимает меры по бесплатному отслеживанию платежной операции и, если это разрешено законом, уведомляет плательщика о результатах.
11. В вопросах, не урегулированных Положениями и условиями, которые касаются ответственности Банка за исполнение платежных поручений, в том числе платежных операций, инициированных через поставщика услуги инициирования платежных операций, и требований о возврате сумм неавторизованных операций, применяются Положения и условия предоставления услуг ING Bank Śląski S.A. в рамках ведения Счета для беженца.
12. При предоставлении услуги Системы Интернет-банкинга в соответствии с настоящими Положениями и условиями, Банк проявляет должную осмотрительность, как это определено в Гражданском кодексе.
13. Банк не несет ответственности за безопасность и работу доверенного мобильного устройства, включая все его функции.

§ 21

Все указания, данные пользователем в системе Интернет-банкинга, постоянно охраняются банком и являются доказательством в случае возникновения спорных ситуаций.

11. Ответственность пользователя

§ 22

1. Банк проявляет должную заботу с точки зрения Гражданского кодекса при предоставлении услуги системы Интернет-банкинга в соответствии с настоящими Положениями и условиями.

2. Банк не несет ответственности за безопасность и работу доверенного мобильного устройства, включая все его функции.

§ 22 a

1. Пользователь обязуется не предпринимать никаких действий, которые могут привести к получению доступа к Системе третьими лицами, даже если это другой пользователь.
2. Пользователь обязан соблюдать следующие правила пользования Системой:

1) сохранять конфиденциальность всех данных и информации, предназначенных для:

a) аутентификации и авторизации всех распоряжений (платежных или неплатежных) (например, логин, коды, пароль, PIN-код), которые предназначены для использования Системы или любой ее части,

b) использования Системы, приложения «Мой ING» или их функций или возможностей.

Эти данные и информация не должны передаваться пользователем третьим лицам, даже если это лицо является другим авторизованным пользователем услуг через Систему,

2) запомнить свой пароль или другие данные, используемые для аутентификации и авторизации, и, если он не может этого сделать, хранить этот пароль и данные в безопасном месте по своему выбору и в защищенном месте, недоступном для третьих лиц. Пользователь обязан хранить устройства для входа в систему, аутентификации или авторизации (например, ключ U2F) таким же образом. Недопустимо хранить пароль и данные, обеспечивающие аутентификацию или авторизацию, в одном месте (например, хранить пароль вместе с другими данными),

3) пользователь обязуется не предоставлять третьему лицу доверенное мобильное устройство, которое позволит третьему лицу получать данные аутентификации или авторизации или выдавать распоряжения через Систему,

4) пользователь обязуется:

a) не устанавливать и не разрешать установку на своем доверенном устройстве или другом устройстве, которое использует пользователь для подключения к Системе, какого-либо программного обеспечения или инструмента, который позволит третьему лицу получить доступ к Системе, и

b) не подключать к доверенному устройству или любому другому устройству, которое пользователь использует для подключения к Системе, программное обеспечение, которое позволит другим лицам/субъектам получить доступ к Системе, включая получение контроля над устройством пользователя или управление его функциями (любые способы выдать себя за пользователя),

5) пользователь обязуется защищать доверенное устройство и устройства, которые пользователь использует для подключения к Системе (например, компьютер, мобильный телефон, другие мобильные устройства), от вредоносных программ или доступа третьих лиц путем:

a) установки только легального программного обеспечения на доверенном устройстве и других устройствах, с которых пользователь подключается к Системе,

b) установки антивирусного программного обеспечения, с учетом того, что оно может быть бесплатным на доверенном устройстве и других устройствах, с которых пользователь подключается к Системе,

c) установки кода, пароля или PIN-кода или другой меры безопасности для доступа к доверенному устройству или другому устройству, с которого пользователь подключается к Системе,

d) запрета хранить биометрические признаки третьих лиц на доверенном или другом устройстве, используемом для аутентификации или авторизации, например, черты лица (функция face ID) или отпечатки пальцев, рисунок сосудов (функция touch ID), поскольку это создает риск того, что устройство классифицирует данные третьих лиц как данные пользователя,

6) пользователь обязуется регулярно устанавливать обновления (в том числе новые версии и патчи) мобильного приложения – не позднее сроков, указанных Банком. В случае если обновление, новая версия или патч являются критическими, Банк уведомляет пользователя о необходимости их установки и внедрения непосредственно перед входом в систему. Кроме того, если пользователь установил мобильное приложение или постоянно использует одно и то же устройство во время работы с Системой, он обязан регулярно обновлять и устанавливать патчи и новые версии, как минимум программного обеспечения операционной системы (например, Android, iOS), которые рекомендуются производителями устройств или программного обеспечения, если соответствующий производитель обеспечивает такую поддержку. Отсутствие установки актуальных версий или патчей вышеперечисленного может повлиять на безопасность Системы.

3. Пользователь должен соблюдать следующие правила, касающиеся аутентификации и

авторизации распоряжений:

1) перед каждой авторизацией пользователь обязан проверить, соответствует ли распоряжение намерениям пользователя, а если пользователь получает информацию от Банка перед авторизацией, он обязан ознакомиться с этой информацией. Если распоряжение предусматривает добавление устройства в перечень доверенных устройств, пользователь должен убедиться, что он действительно имеет такое устройство (фактически владеет им), прежде чем отправлять распоряжение,

2) пользователь обязан незамедлительно сообщать Банку о любых несанкционированных, неправильно инициированных, неисполненных или ненадлежащим образом исполненных платежных операциях в результате распоряжений, отправленных с помощью Системы. Такое уведомление может быть сделано пользователем через Систему, по телефону инфолинии или в отделении банка,

3) если пользователь намерен использовать метод аутентификации или авторизации, основанный на биометрическом идентификаторе, он должен использовать только одну собственную биометрическую характеристику, которая является основой для создания биометрического идентификатора. Если мобильное устройство позволяет регистрировать несколько копий биометрической характеристики (например, отпечатки нескольких пальцев), пользователь обязан регистрировать только одну свою биометрическую характеристику, поскольку эта характеристика будет присвоена ключу пользователя, упомянутому в § 1 абз. 2 пункт 5).

4. Пользователь также обязан немедленно сообщить Банку о потере, краже,

незаконном присвоении или несанкционированном использовании данных аутентификации или авторизации

в Системе, а также несанкционированном доступе к Системе.

5. Пользователь также обязан незамедлительно уведомить Банк в случае

обнаружения:

1) потери, кражи, незаконного присвоения или обнаружения несанкционированного использования доверенного устройства или мобильного телефона или другого устройства, связанного с телефонным номером, помеченным как телефонный номер для аутентификации, или устройством для входа, аутентификации или авторизации (например, ключ U2F),

2) любого технического инцидента или иного сбоя, связанного с использованием Системы, который, по мнению Пользователя, может поставить под угрозу безопасность Системы или безопасное использование Системы пользователем,

3) что третьи лица пытались войти в Систему. Пользователь также обязан незамедлительно уведомить Банк, если, по его мнению, есть обоснованные подозрения в нарушении безопасности или конфиденциальности используемых им индивидуальных аутентификационных данных, таких как коды, коды авторизации или биометрические идентификаторы.

6. В случаях, указанных в абз. 4 или абз. 5, а также в случае обнаружения или подозрения,

что третьим лицам были переданы данные аутентификации или авторизации

распоряжения или доступа к Системе другими лицами, пользователь должен немедленно:

1) уведомить Банк и заблокировать доступ к Системе или поручить Банку заблокировать доступ к Системе. Распоряжение о блокировке Системы можно выдать в отделении банка, осуществляющем это действие, через Систему или через инфолинию,

2) изменить все данные аутентификации или авторизации, которые могут быть изменены.

7. В случае, если пользователь обнаружит, что:

1) было совершено преступление, включая кражу личности, или действие, повлекшее за собой доступ к Системе неавторизованного лица, или

2) имело место использование третьим лицом других платежных инструментов или данных, к которым доступ предоставляется Системой или любой ее частью, или

3) получение третьими лицами биометрических характеристик или биометрических идентификаторов, записанных на доверенном мобильном устройстве, может привести к несанкционированному доступу таких лиц к мобильному приложению и несанкционированной авторизации распоряжений – пользователь обязан незамедлительно принять меры, предусмотренные в абз. 5, и заблокировать соответствующие данные или номера платежных инструментов в соответствующих учреждениях. Кроме того, в случае подозрения в совершении преступления пользователь обязан сообщить об этом в компетентный орган, в частности в прокуратуру или полицию.

8. Положения о доступе третьих лиц к Системе не применяются в случае:

1) если провайдер, предоставляющий услугу инициирования платежной операции, или провайдер, предоставляющий услугу доступа к информации о счете, действует от имени пользователя, при условии, что эти провайдеры действуют с согласия пользователя с целью и в пределах выполнения этих услуг,

2) если другим пользователем системы является несовершеннолетний, от имени которого пользователь, являющийся законным представителем этого несовершеннолетнего, заключил договор на использование Системы. Вышеизложенное не нарушает принцип, согласно которому каждый пользователь может давать только собственные распоряжения, а несовершеннолетний может давать распоряжения только в той мере, в какой он уполномочен на это своим законным представителем или имеет право по закону.

9. Чтобы ограничить риск использования пользователем сайтов, похожих на сайт Банка, пользователь обязан при входе в систему проверять, имеет ли отображаемая страница сертификат сайта Банка. Способ проверки данного сертификата является общедоступной информацией и указан на сайте Банка и на странице входа в Систему Банка. Для справки приводим текущее название сайта Банка – www.ing.pl. Название сайта может быть изменено, о чем Банк сообщит в Сообщении.

10. Пользователь не должен:

1) входить в систему с доверенного устройства или любого другого устройства, которое он постоянно использует при посещении веб-сайтов, помеченных как небезопасные или опасные (в таких случаях производители программного обеспечения также практикуют вывод на устройство пользователя

сообщения рядом с названием искомого веб-сайта, например, «соединение небезопасно» или знак/значок «!»),

2) легковерно разрешать приложениям, установленным на доверенном устройстве или устройстве, которое пользователь регулярно использует при работе с Системой, получать доступ к другим приложениям, а также к своим фотографиям, видеозаписям или контактам, – поскольку такая практика повышает риск несанкционированного доступа к доверенному устройству или устройству, которое пользователь регулярно использует при работе с Системой.

11. Пользователь может направлять заявки или уведомления, указанные в Положениях и условиях, через Систему, по телефону инфолинии или в банковском учреждении.

§ 22b

1. Банк рассматривает заявку пользователя о неавторизованной операции и проводит всестороннее расследование обстоятельств, связанных с операцией. Цель расследования – определить, правильно ли было подано распоряжение пользователя и авторизовал ли он его. Расследование также включает определение того, является ли распоряжение распоряжением пользователя или оно было сделано третьим лицом, в том числе с помощью программного обеспечения или другого устройства.

2. Если выяснится, что плательщик не давал согласия на совершение операции, считается, что такое распоряжение не было авторизовано. Вышеизложенное не противоречит правилам ответственности, описанным в настоящих Положениях и условиях.

§ 22c

1. Если пользователь нарушает одно или несколько обязательств, описанных в § 22a, считается, что пользователь использует Систему не в соответствии с Положениями и условиями.

2. Пользователь несет ответственность за несанкционированные операции в полном объеме, если они явились результатом умышленного или грубого нарушения хотя бы одного из обязательств пользователя согласно § 22a абз. 1-9.

3. За исключением абз. 2, ответственность пользователя за неавторизованные операции ограничивается эквивалентом суммы 50 евро в польской валюте, пересчитанной по среднему курсу евро, опубликованному Национальным банком Польши (NBP), действующему на день совершения операции, если неавторизованная операция является результатом:

1) использования данных аутентификации или авторизации, утерянных пользователем или украденных у него,

2) неправомерного присвоения данных аутентификации или авторизации третьим лицом.

Пользователь не несет ответственности за неавторизованные операции, если:

3) он не мог установить факт потери, кражи или незаконного присвоения данных аутентификации или авторизации до совершения платежной операции, за исключением случаев, когда пользователь действовал умышленно, или

4) потеря данных аутентификации или авторизации до совершения операции была вызвана действием или бездействием Банка или организаций, указанных в статье 6 пункт 10 Закона о платежных услугах.

4. За исключением ситуаций, описанных в абз. 2 и 3, в случае неавторизованной операции Банк возмещает сумму неавторизованной операции плательщику немедленно – но не позднее конца рабочего дня, следующего за днем обнаружения неавторизованной операции или днем получения уведомления – за исключением случаев, когда у Банка есть разумные и должным образом задокументированные основания подозревать мошенничество и письменно информировать об этом органы, уполномоченные преследовать преступления. Если плательщик использует платежный счет, а возврат средств в соответствии с вышеуказанным правилом подлежит возмещению, Банк восстанавливает дебетованный счет до состояния, в котором он находился бы, если бы не было неавторизованной платежной операции.

5. Плательщик не несет ответственности за неавторизованные операции после сообщения Банку об утере, краже, присвоении или несанкционированном использовании данных, используемых для аутентификации

или авторизации в Системе, а также о несанкционированном доступе к Системе, как указано в § 22a, абз. 4, если он не действовал умышленно.

6. Если операция была неавторизованной и Банк не требовал от пользователя строгой аутентификации, пользователь не несет ответственности за неавторизованные платежные операции, если только он не действовал умышленно. Вышесказанное не относится к случаям, когда Банк имел законное право отказаться от требования строгой аутентификации. Если получатель платежа или поставщик получателя платежа не принимает строгую аутентификацию пользователя, они несут ответственность за ущерб, понесенный Банком.
7. Несмотря на вышесказанное, если пользователь не сообщит о неавторизованных, неправильно инициированных, неисполненных или ненадлежащим образом исполненных платежных операциях в течение 13 месяцев с даты списания средств со счета или даты, когда операция должна была быть исполнена, претензии пользователя в отношении неавторизованных, неисполненных или ненадлежащим образом исполненных платежных операций теряют силу.

§ 22d

1. Если пользователь нарушит одно или несколько обязательств, указанных в § 22 или § 22a, и если в результате этого нарушения будет установлено, что:
   1) третье лицо, используя все или часть данных пользователя для аутентификации или авторизации – дало или санкционировало неплатежное распоряжение, а Банк исполнил это распоряжение или сделал соответствующее заявление (например, при заключении договора), и
   2) Банк понес ущерб в результате выполнения распоряжения или предоставления соответствующей выписки, поскольку распоряжение исходило не от пользователя,

   то пользователь обязан возместить ущерб, причиненный Банку в результате нарушения обязательств, предусмотренных § 22 и § 22a, в зависимости от степени нарушения этих обязательств.
2. Ответственность пользователя ограничивается фактическим ущербом Банка, возникшим в результате нарушения обязательств, предусмотренных § 22 и 22a. Ответственность пользователя не лишает Банк права требовать возмещения ущерба от третьей стороны до тех пор, пока ущерб не будет полностью возмещен.

12. Прочие правила и рекомендации по безопасному использованию системы

§ 23

1. Банк уведомляет пользователя о существующих угрозах, т.е. о случаях мошенничества или подозрениях на мошенничество или других рисках безопасности использования Системы. Эти уведомления могут:
   1) передаваться пользователю перед входом в Систему,
   2) передаваться пользователю в Системе (например, после входа в систему, в сообщениях),
   3) передаваться по другому защищенному каналу связи, согласованному между пользователем и Банком.

   Кроме того, информация по этому вопросу публикуется на сайте Банка.
2. Пользователь обязан ознакомиться с предупреждениями о рисках, упомянутыми в абз. 1, и должен соблюдать указанные в них рекомендации. Если вы не ознакомитесь с уведомлениями о рисках и не будете следовать рекомендациям, это может привести, в частности, к риску:
   1) возникновение социально-технических атак, в ходе которых третьи лица могут – выдавая себя за Банк или другое учреждение – побудить пользователя предоставить идентификационные данные, коды авторизации или PIN-коды,
   2) авторизации пользователем распоряжения, которое он не давал,
   3) использования устройств, контроль над которым перешел к третьим лицам.

3. Пользователям рекомендуется убедиться в том, что их компьютерная среда и среда мобильных устройств безопасны. Пользователь обязан применять действующие рекомендации Банка по безопасности операций в Интернете защиты от конкретных угроз, возникающих при подключении к Интернету. Эти рекомендации представлены Банком на веб-сайте Банка.

   Информация о последующих обновлениях этих рекомендаций рассылается через Систему.

4. Банк применяет меры безопасности, которые снижают риск несанкционированного использования мобильного приложения. В связи с этим Банк имеет право использовать электронные механизмы для проверки того, внес ли пользователь или третье лицо изменения в доверенное мобильное устройство или в оригинальное программное обеспечение, требуемое производителем, которое было установлено на устройстве. Следует признать, что внесение вышеуказанных изменений может привести к риску получения контроля над устройством неуполномоченным лицом.

5. Если Банк определяет, что существует риск получения контроля над доверенным устройством неуполномоченным лицом, Банк может снизить лимит операций для платежных распоряжений в мобильном приложении, выполненных с этого устройства – в крайнем случае до 95% от суммы лимита, установленного Положениями и условиями. Банк немедленно уведомит об этом пользователя. Банк имеет право заблокировать Систему в соответствии с § 27 абз. 2, если вышеуказанный риск становится высоким или Банк определяет, что с устройства, контроль над которым, вероятно, захвачен неуполномоченным лицом, подаются дальнейшие платежные распоряжения или другие распоряжения, что может привести к несанкционированному доступу третьих лиц к счетам, продуктам или банковским услугам, использующим Систему.

§ 24

1. Банк публикует информацию о безопасном использовании Системы на веб-сайте Банка и внутри Системы. Подробную информацию о том, где публиковать информацию и рекомендации по безопасности, можно найти в Объявлении.

2. Для входа в систему Интернет-банкинга и ее использования по запросу пользователя требуются файлы cookie или другие технологии, которые исходят от этой Системы. Банк использует файлы cookie и другие технологии в соответствии со своей Политикой использования файлов cookie (далее – Политика использования файлов cookie). В системе Интернет-банкинга файлы cookie и другие технологии используются для установления и поддержания сеанса пользователя в системе, для защиты целостности транзакций, а также для определения технических и технологических характеристик устройства, используемого при пользовании услугами системы, в связи с требованиями безопасности системы и выполняемых транзакций. Если пользователь использует веб-сайт Банка, а не систему Интернет-банкинга, он может, в соответствии с Политикой Банка в отношении файлов cookie, настроить свой Интернет-браузер таким образом, чтобы не принимать файлы cookie, отличные от тех, которые используются в Системе. Политика Cookie, применяемая Банком, доступна на веб-сайте Банка.

3. Пользователь обязан незамедлительно уведомлять Банк о любых изменениях в личных данных и контактной информации пользователя. Изменение данных может быть подано с помощью системы Интернет-банкинга при условии, что в системе есть технические возможности для такого изменения данных. За исключением случаев, когда пользователь подает документ в форме нотариального акта, подлинность подписи пользователя должна быть засвидетельствована:

   1) нотариусом – в случае документов, подписанных в Республике Польша;

   2) польским дипломатическим представительством, консульским учреждением или нотариусом страны, с которой Республика Польша подписала соглашение о правовой помощи по гражданским делам, или подтверждено официальным лицом или нотариальной конторой и сопровождено апостилем в смысле Конвенции – в случае документов, подписанных за границей.

4. За исключением абз. 5, распоряжения, данные по переписке, должны быть в форме, указанной в абз. 3.

5. Заявления пользователя, указанные в § 29 абз. 1, § 31 абз. 3, могут быть отправлены по почте без соблюдения условий, предусмотренных в абз. 3. Однако Банк оставляет за собой право провести дополнительную проверку представленных заявлений.

§ 25

1. Систему Интернет-банкинга можно разблокировать, подав распоряжение в отделении банка, осуществляющем данную деятельность, заполнив соответствующее заявление на веб-сайте банка или в мобильном приложении, при условии, что банк разрешает такую функциональность. Использование Системы будет возможно после повторного назначения пароля или PIN-кода для мобильного приложения.
2. Пользователь может изменить существующие данные, необходимые для получения аутентификации или авторизации:

   1) через Систему – при наличии существующего телефона для авторизации,

   2) подав соответствующее распоряжение на веб-сайте или в отделении банка – если у него нет существующего номера телефона для авторизации.

§ 26

1. В целях безопасности мобильное устройство, предназначенное для использования всех функций мобильного приложения, должно быть добавлено в перечень доверенных мобильных устройств. Если одно мобильное устройство указано как доверенное несколькими пользователями, каждый из этих пользователей обязан соблюдать требования безопасности, предусмотренные Положениями и условиями, включая безопасное прекращение использования приложения.
2. Перечень доверенных мобильных устройств доступен в Системе.
3. Мобильное устройство можно исключить из перечня в системе Интернет-банкинга или в мобильном приложении. Банк имеет право удалить мобильное устройство из перечня, если у него есть обоснованные сомнения в том, что пользователь не использует устройство или что доступ к устройству получило неуполномоченное лицо. Предполагается, что пользователь не использует мобильное устройство, если он не входил в мобильное приложение с этого устройства в течение 90 дней. Пользователь может снова добавить устройство в перечень. В зависимости от версии мобильного приложения, удаление из перечня может также произойти автоматически в результате активации приложения на другом устройстве в целях безопасности.
4. Доверенный браузер можно удалить из списка в системе Интернет-банкинга. Банк имеет право удалить доверенный браузер из списка, если у него есть обоснованные сомнения в том, что пользователь не использует устройство или что доступ к устройству был получен неуполномоченным лицом. В целях безопасности доверенный браузер будет удален из списка по истечении 90 дней с момента его добавления в список доверенных браузеров. Пользователь может снова добавить нужный браузер в список.
5. Удаление ключа безопасности из списка ключей возможно в Системе банкинга, если предварительно была выполнена аутентификация с использованием ключа безопасности в отделении банка или по телефону его инфолинии.
6. В случае потери, кражи, незаконного присвоения или несанкционированного использования доверенного мобильного устройства, пользователь должен как можно скорее удалить подозреваемое устройство из перечня в соответствии с абз. 3.
7. В случае подозрения на несанкционированное использование Системы или кражу, хищение устройства, к которому подключен телефон авторизации, или подозрения на умышленное проведение несанкционированной сделки, пользователь обязан незамедлительно сообщить об этом Банку посредством Системы Интернет-банкинга или телефона доверия.

§ 27

1. Банк оставляет за собой право проводить модернизацию, обновление и регулярное техническое обслуживание системы Интернет-банкинга, что приводит к периодическим перебоям в доступе к системе или к отдельным функциям. Банк проинформирует пользователя об указанных обстоятельствах, предоставив оценку продолжительности перерыва или ограничения доступа:

   1) с помощью опции сообщения в системе Интернет-банкинга, и/или

2) на домашней странице Банка, и/или

3) по телефону доверия.

2. Банк оставляет за собой право блокировать доступ к системе Интернет-банкинга по соображениям безопасности. Под соображениями безопасности следует понимать ситуации несанкционированного доступа третьих лиц к счетам, продуктам или банковским услугам через Систему или угрозу возникновения такой ситуации, а также в случаях, предусмотренных законом.
3. В случае подозрения на попытку несанкционированного доступа к Системе Банк может приостановить возможность входа в Систему на определенный период времени. Банк проинформирует о том, как снова войти в систему, в сообщении, отправленном на телефон для авторизации.
4. Банк оставляет за собой право отказать в выполнении распоряжения или ввести дополнительные ограничения и гарантии в отношении распоряжений, данных через систему Интернет-банкинга, в случае возникновения важных обстоятельств, препятствующих выполнению распоряжений, т.е. препятствий технологического характера, соображений безопасности или содержания распоряжения, противоречащего действующим в Банке обязательным для пользователя правилам, а также в случае несоблюдения пользователем общепринятых правовых норм.
5. Банк может наложить ограничения на использование системы Интернет-банкинга в случае, если на основании местоположения IP-адреса он определит, что пользователь входит в систему в стране, которая входит в список стран повышенного риска. Список таких стран и степень ограничений подробно описаны на сайте Банка.
6. Банк оставляет за собой право вводить ограничения на использование полной функциональности системы Интернет-банкинга для определенной группы пользователей, находящихся в одинаковой правовой или фактической ситуации. Такие ограничения могут быть обусловлены требованиями безопасности. Банк проинформирует пользователей о введенных ограничениях не менее чем за 14 календарных дней до даты введения указанных ограничений.
7. В целях безопасности Банк имеет право запросить у пользователя обновленные личные данные или подтвердить эти данные.
8. Пользователю запрещается вводить или загружать в Систему любой незаконный контент, а также использовать любые программы, угрожающие другим пользователям Системы или ставящие под угрозу целостность Системы, включая содержащиеся в ней данные или работающие с ней компьютерные приложения. Если определенный сервис Системы, в том числе мобильное приложение, позволяет отображать чужие данные, пользователь не имеет права собирать эти данные и может использовать их только для заказа транзакции
9. В процессе использования Системы Банк может предоставлять пользователю распоряжения по техническим и организационным средствам Системы или объявления об услугах или функциональных возможностях, предоставляемых в рамках Системы. Поручения и объявления носят исключительно информационный характер и не являются рекламой. Они могут передаваться с помощью средств связи, доступных в Системе, или могут быть представлены в графической, текстовой, презентационной или анимационной форме.
10. Получение третьими лицами биометрических характеристик или биометрических идентификаторов, зарегистрированных на доверенном мобильном устройстве, может привести к несанкционированному доступу таких лиц к мобильному приложению и несанкционированной авторизации распоряжений.
11. Для входа в Систему Интернет-банкинга и ее использования по запросу пользователя требуются файлы cookie или другие технологии, которые исходят от этой Системы. Банк использует файлы cookie и другие технологии в соответствии со своей Политикой использования файлов cookie (далее – Политика использования файлов cookie). В системе Интернет-банкинга файлы cookie и другие технологии используются для установления и поддержания сеанса пользователя в системе, для защиты целостности операций, а также для определения технических и технологических характеристик устройства, используемого при пользовании услугами Системы, в связи с требованиями безопасности Системы и проводимых транзакций. Если пользователь использует веб-сайт Банка, а не систему Интернет-банкинга,

он может, в соответствии с Политикой Банка в отношении файлов cookie, настроить свой Интернет-браузер таким образом, чтобы он не принимал файлы cookie, отличные от тех, которые используются в Системе. Политика Банка в отношении файлов cookie размещена на веб-сайте Банка.

13. Технические требования к использованию системы

§ 28

1. Пользователь может использовать Систему после выполнения следующих минимальных технических требований: наличие электронного устройства, в частности компьютера, мобильного телефона или другого мобильного устройства с доступом в Интернет, операционной системы и Веб-браузера, установленных на этом устройстве. В случае намерения использовать функции, поддерживаемые отдельными приложениями, например, мобильным приложением, необходимо установить такое приложение на мобильное устройство.
2. В течение срока действия Договора Пользователь обязан указать телефон для авторизации и иметь в своем распоряжении последний указанный телефон. Отсутствие указания телефона для авторизации делает невозможным использование Системы или ее отдельных функций.
3. Технические требования, связанные с коммуникацией между пользователем и Системой:

   1) для Интернет-банкинга – операционные системы Apple OS X и Windows

   2) для мобильного приложения – операционные системы iOS и Android.

   Дополнительная информация, касающаяся связи пользователя с Системой или с конкретными приложениями, программами, типами файлов или касающаяся Веб-браузеров и их версий и версий операционных систем, указывается в Объявлении и на веб-сайте Банка.
4. В связи с техническим и технологическим развитием отдельные версии Системы могут быть обновлены, улучшены, изменены или заменены новыми версиями. Насколько это технически возможно, обновления или улучшения могут производиться во время работы Системы. В случае, если любая из вышеперечисленных операций требует от пользователя перезапуска или установки пользователем новой версии Системы, Банк информирует об этом пользователя с помощью соответствующих экранов, уведомлений или сообщений.
5. Банк может отозвать старую версию Системы, заменив ее более новой. В этом случае пользователь должен быть заблаговременно проинформирован о предполагаемой дате замены старой версии на более новую и о необходимых действиях, если таковые потребуются, в той мере, в какой эти действия будут необходимы пользователю по техническим причинам, в частности, для загрузки и установки новой версии или для выполнения этих действий на определенном типе устройства.

14. Расторжение, уведомление и истечение срока действия договора

§ 29

1. Клиент имеет право расторгнуть Договор с немедленным вступлением в силу, без уведомления. Распоряжение о расторжении Договора может быть подано в письменной форме под страхом недействительности или через систему Интернет-банкинга, если Система позволяет такой способ подачи заявления о расторжении Договора.
2. Банк имеет право расторгнуть заключенный с клиентом Договор, предупредив его за два месяца до расторжения.
3. Банк имеет право расторгнуть заключенный с Клиентом Договор с соответствующим и установленным сроком уведомления в следующих случаях (уважительные причины для расторжения Договора путем уведомления):

   1) Банк определил, что пользователь не соблюдает правила безопасного использования Системы, описанные в главе 13 настоящих Положений и условий,

2) Банк получил информацию, составляющую обоснованное подозрение, что Пользователь совершил преступление с использованием Системы Интернет-банкинга или преступление в ущерб Банку,

3) непредоставление пользователем, как указано в Положениях и условиях, информации, необходимой для активации данной услуги или необходимой для продолжения предоставления услуги системы Интернет-банкинга,

4) предоставление пользователем данных или информации, не соответствующих действительности или не соответствующих фактам, включая использование устаревших документов (в том числе документов, срок действия которых истек), фальшивых, поддельных или контрафактных документов,

5) неспособность Банка выполнить свои обязательства по применению мер финансовой безопасности, предусмотренных Законом «О ПОД/ФТ».

4. Договор расторгается в случае смерти клиента. Факт смерти может быть подтвержден достоверным документом, в частности:

1) полной или сокращенной копией свидетельства о смерти,

2) свидетельством о смерти,

3) письмом из пенсионного органа,

4) справкой из регистра Государственной электронной системы регистрации населения (PESEL),

5) письмом из полиции, из суда, от судебного исполнителя,

6) любым другим достоверным документом, подтверждающим смерть клиента.

В случае если документ вызывает сомнения, в частности, в отношении его подлинности или подтверждения факта или даты смерти пользователя, или имеются другие существенные обстоятельства, которые приводят к сомнениям в отношении факта или даты смерти пользователя, Банк рассматривает полную или сокращенную копию свидетельства о смерти в качестве документа, подтверждающего факт смерти, если решением суда или законом не предусмотрено иное.

15. Жалобы. Разрешение споров

§ 30

1. В вопросах жалоб, касающихся платежных распоряжений, предусмотренных настоящими Положениями и условиями, но относящихся к счетам, регулируемым Положениями и условиями счетов для розничных клиентов, применяются положения того из этих Положений и условий, которое применимо к данному счету. Право условного кредитования счета или списания с него суммы, возникшей в результате жалобы, которое предоставляется пользователем в соответствии с договором счета, распространяется также на операции, возникшие в результате платежных поручений, предусмотренных настоящими Положениями и условиями. Вспомогательная информация по счетам, на которые распространяется действие Положений и условий о счетах для розничных клиентов, в зависимости от ситуации.
2. Подача претензии в отношении несанкционированных, неправильно инициированных или ненадлежащим образом исполненных или неисполненных распоряжений, которые были даны Системой, должна быть сделана незамедлительно, но не позднее 13 месяцев с даты, оспариваемой распоряжения.
3. С учетом положений § 22 и § 22a, в случае платежной операции, несанкционированной лицом, уполномоченным распоряжаться счетом, Банк немедленно возвращает деньги – однако не позднее конца рабочего дня, следующего за днем, в который было установлено, что со счета плательщика была списана несанкционированная операция, или днем, в который Банк получил соответствующее уведомление, за исключением случаев, когда провайдер плательщика имеет разумные и надлежащим образом документированные основания подозревать мошенничество и письменно информирует органы, назначенные для преследования преступлений, о сумме несанкционированной платежной операции и восстанавливает дебетованный счет до состояния, в котором он находился бы, если бы несанкционированная платежная операция не состоялась.
4. Пользователь имеет право подать жалобу. Жалоба может быть подана:

1) в электронной форме:

a) через систему Интернет-банкинга,

b) по адресу электронной доставки, зарегистрированному в базе электронных адресов AE:PL-69368-51081-ERVRU-12, в той мере, в какой услуга регистрируемой электронной доставки активирована в соответствии с действующими правовыми нормами и договорами, заключенными между владельцем депозитного счета и банком;

2) в устной форме:

a) по телефону по номерам, указанным на сайте Банка (стоимость звонка согласно тарифам оператора),

b) лично в банковском отделении, осуществляющем данную операцию;

3) в письменной форме:

a) по почте на адрес Банка, указанный на веб-сайте Банка,

b) лично в банковском отделении, осуществляющем данную операцию.

5. В обоснованных случаях жалобы, поданные через систему Интернет-банкинга или по телефону через инфолинию по поводу несанкционированных, неправильно начатых, невыполненных или ненадлежащим образом выполненных платежных операций или распоряжений, должны быть дополнительно подтверждены пользователем в письменном виде в отделении банка, осуществляющем данную деятельность, в течение 14 календарных дней, считая со дня подачи жалобы.

6. Банк обязан предоставить ответ на жалобу:

1) в электронной форме:

a) через систему Интернет-банкинга,

b) на электронный адрес доставки, указанный держателем, при условии, что Банк в состоянии ответить на него по этому адресу,

или одним из следующих способов, выбранных клиентом:

2) на бумаге – либо в отделении банка, осуществляющем такую деятельность, либо письмом на адрес для корреспонденции,

3) на другом долговечном носителе, если стороны договорятся об этом.

7. Банк должен ответить как можно скорее, но не позднее 15 рабочих дней (для жалоб, связанных с платежными услугами) и 30 дней (для жалоб, не связанных с платежными услугами) с даты получения жалобы. В ходе рассмотрения жалобы Банк может запросить дополнительную информацию или документы. В особо сложных случаях, не позволяющих рассмотреть жалобу и ответить на нее в указанный срок, срок может быть продлен, но не может превышать 35 рабочих дней (для жалоб, связанных с платежными услугами) и 60 дней (для жалоб, не связанных с платежными услугами) с момента получения жалобы. Банк проинформирует пользователя о причинах задержки, укажет обстоятельства, которые необходимо установить для рассмотрения жалобы, предполагаемую дату завершения процедуры рассмотрения жалобы.

8. В ходе рассмотрения жалобы Банк может попросить пользователя предоставить дополнительные объяснения или документы. В случае необходимости выяснения дополнительных обстоятельств в связи с рассмотрением жалобы, Банк оставляет за собой право связаться с пользователем по номеру телефона, указанному пользователем для связи с Банком.

9. Если Банк не принимает жалобу, пользователь имеет право подать апелляцию. Если пользователю известны новые, относящиеся к делу факты, обстоятельства или доказательства, он обязан сообщить их Банку в запросе. Банк повторно рассматривает жалобу в сроки, установленные для рассмотрения жалоб. Если в результате рассмотрений жалобы между клиентом и Банком возникает спор, он может быть решен мирным путем, путем заключения мирового соглашения.

10. Все споры, возникающие из Договора, заключенного между Банком и пользователем, могут быть разрешены во внесудебном порядке. Заявки можно подавать на имя:

1) Финансового омбудсмена, веб-сайт: www.rf.gov.pl. Омбудсмен действует в соответствии с Законом «О рассмотрении жалоб операторами финансового рынка, о финансовом омбудсмене и Фонде финансового образования,

2) Банковского арбитра, действующего при Ассоциации польских банков, веб-сайт: www.zbp.pl/dla-konsumentow/arbiter-bankowy/dzialalnosc. Арбитр должен разрешить спор и вынести свое решение в соответствии с Правилами банковского потребительского арбитража.

11. Даже если пользователь использует платформу ODR, он все равно можете подать заявление банковскому арбитру или финансовому омбудсмену. Банк также может подать запрос на внесудебное разрешение спора против пользователя через платформу ODR – если обе стороны заранее согласны на это и правила организации ODR и закон не исключают такую возможность.

12. Пользователь также может обратиться за помощью к омбудсмену по защите прав потребителей (муниципальному или районному).

13. Споры, возникающие в связи с Договором, также могут быть разрешены в судебном порядке. Компетентным судом для рассмотрения любых споров является суд, определенный в соответствии с положениями Гражданского процессуального кодекса.

14. Пользователь может подать жалобу в орган, осуществляющий надзор за банком (Управление финансового надзора) на действия банка, если, по мнению пользователя, эти действия нарушают закон, а также в случае отказа в предоставлении платежных услуг пользователю.

16. Поправки к Положениями и условиям

§ 31

1. Банк оставляет за собой право вносить изменения в Положения и условия по важным причинам. Ниже перечислены важные причины, которые приводят к необходимости внесения изменений в Положения и условия в той степени, в какой это необходимо и которая вытекает из данной причины:

   1) введение нового или измененного законодательства, регулирующего предоставление услуг Банком или регулирующего использование таких услуг пользователем,

   2) выдача решения, рекомендации, указания, позиции, постановления или любого другого документа органом надзора или иным уполномоченным субъектом, определяющего положения и условия оказания услуг Банком или устанавливающего положения и условия пользования этими услугами владельцем счета по договору, заключенному с ним,

   3) расширение, изменение или ограничение функциональности услуг, изменение положений и условий пользования услугами пользователем, введение новых услуг, отказ от совершения определенных видов деятельности, являющихся предметом услуг, оказываемых Банком в рамках заключенного с пользователем договора,

   4) изменения в ИТ-системе Банка в результате:

      a) совершенствования ИТ-систем Банка в связи с развитием технологий,

      b) обязательных изменений, вносимых в системы межбанковских расчетов в отношении участников этих систем,

      c) смены поставщиков программного обеспечения, приводящей к изменениям в функциональности ИТ-системы Банка,

   - затрагивающие услуги, предусмотренные настоящими Положениями и условиями, предоставляемые Банком, или на условия использования пользователем этих услуг в рамках заключенного с ним договора.

2. Банк уведомляет пользователя об изменениях в Положениях и условиях в порядке, согласованном с пользователем и указанном в § 32 абз. 2, не позднее, чем за два месяца до предполагаемой даты вступления в силу изменений в Положениях и условиях.

3. Пользователь имеет право до даты предполагаемого вступления в силу изменений:

1) расторгнуть Договор без взимания платы со дня информирования его об изменениях, но не позднее даты, когда изменения вступят в силу,

2) подать возражение против предлагаемых изменений.

Если пользователь не возражает против изменений в письменной форме до предполагаемой даты вступления в силу, считается, что пользователь согласен с изменениями. В случае если пользователь подаст возражение, но не расторгает Договор, Договор прекращает свое действие в день, предшествующий дате вступления в силу предлагаемых изменений, без взимания платы.

4. Изменения функциональных возможностей Системы или отдельных услуг, связанные с техническим/технологическим развитием, не требуют внесения изменений в настоящие Положения и условия при условии, что они не изменяют условия предоставления услуг пользователю в рамках заключенного с ним Договора.
5. До предполагаемой даты вступления в силу изменений в Положениях и условиях Банк может разрешить пользователю воспользоваться изменениями в существующих услугах или использовать новые услуги при условии, что пользователь принимает изменения в Положениях и условиях, относящиеся к соответствующей услуге.

17. Заключительные положения

§ 32

1. С Положениями и условиями можно ознакомиться в отделениях Банка и на веб-сайте Банка.
2. Банк уведомляет клиента о любых изменениях в Положениях и условиях в форме уведомления, отправленного на долговечном носителе:
   1) через систему Интернет-банкинга, или
   2) любым другим способом, согласованным сторонами.
3. Названия глав приведены исключительно в информационных целях, чтобы облегчить понимание текста Положений и условий.
4. Положения и условия вступают в силу с 15 Маршировать 2025 года.

Приложении 1

РЕЖИМ РЕАЛИЗАЦИИ ПЛАТЕЖНЫХ ПОРУЧЕНИЙ И ДРУГИХ РАСПОРЯЖЕНИЙ через Систему Интернет-БАНКИНГА

Предельное время приемки платежных поручений через Систему Интернет-банкинга зависит от времени работы банковских систем, что отражено в нижеуказанной таблице. Платежное поручение, внесенное через Систему Интернет-банкинга после предельного времени, считается полученным в первый рабочий день, последующий за днем внесения этого поручения.

Режим реализации платежных поручений, касающихся поручения на перевод, постоянного платежного поручения:

Предельное время приемки платежных поручений	**Вид платежного поручения**	
	С текущей датой реализации	**С отсроченной датой реализации** <u>независимо от времени подачи поручения</u>
отсутствует поручение, выполняемое в режиме реального времени	Поручения, которые не требуют конвертации валюты	
	a) поручение на внутренний перевод в PLN или перевод в рамках услуги «Плати с ING» b) поручение на внутренний перевод в иностранной валюте, внутренний перевод, c) внесенный как перевод Express ELIXIR или перевод BlueCash	a) поручение на внутренний перевод в PLN b) поручение на внутренний перевод в иностранной валюте c) постоянное поручение на счете в банке
Отсутствует поручение, выполняемое в соответствии с графиком расчетных сессий банка	Поручения, которые не требуют конвертации валюты	
	a) перевод внутри страны, в том числе внесенный в качестве перевода в рамках услуги «Плати с ING»	a) перевод внутри страны b) постоянное поручение на счете в других банках
15:00 (с понедельника по пятницу)	Поручения, которые требуют и не требуют конвертации валюты	
	a) перевод TARGET	a) перевод TARGET
17:00 (с понедельника по пятницу)	Поручения, которые не требуют конвертации валюты	
	a) валютный перевод за пределами страны b) поручение на перевод SEPA c) поручение на перевод в иностранной валюте	a) валютный перевод за пределами страны b) поручение на перевод SEPA c) поручение на перевод в иностранной валюте
	Поручения, которые требуют конвертации валюты	
	a) перевод внутри страны b) валютный перевод за пределами страны c) поручение на перевод SEPA d) поручение на перевод в иностранной валюте	a) перевод внутри страны b) валютный перевод за пределами страны c) поручение на перевод SEPA d) поручение на перевод в иностранной валюте
19:00 (с понедельника по пятницу)	Поручения, которые требуют конвертации валюты	
	a) поручение на внутренний перевод в PLN b) поручение на внутренний перевод в иностранной валюте	a) поручение на внутренний перевод в PLN b) поручение на внутренний перевод в иностранной валюте

ОТМЕНА ПЕРЕВОДОВ ЧЕРЕЗ ИНТЕРНЕТ-БАНКИНГ

Вид перевода, который можно отменить – с текущей датой реализации	Когда можно отменить перевод
Пользователь может отменить в Системе Интернет-банкинг перевод денежных средств с текущих сберегательно-расчетных счетов, за исключением переводов с текущей датой реализации инициированных поставщиком, предоставляющим услуги инициирования платежной транзакции	
• перевод внутри страны , который не требует конвертации и не реализуется в режиме реального времени и не вносится как перевод в рамках услуги «Плати с ING»	• внесенный **с 00:01 до 8:15 с понедельника по пятницу**, может быть отменен до 9:00 в день подачи перевода • внесенный **с 8:16 до 11:35 с понедельника по пятницу**, может быть отменена до 13:00 в день подачи перевода • внесенный **с 11:36 до 14:45 с понедельника по пятницу**, может быть отменена до 15:30 в день подачи перевода • внесенный **с 14:46 до 24:00 с понедельника по пятницу**, может быть отменен до 9:00 ближайшего рабочего дня • внесенный **с 00:01 до 24:00 в субботу, воскресенье или в нерабочий день Банка**, может быть отменен до 9:00 ближайшего рабочего дня
• перевод TARGET • перевод внутри страны, который требует конвертации на валюту • перевод валюты за пределами страны • поручение на перевод SEPA • поручение на перевод в иностранной валюте	• внесенный **с 17:01 до 24:00 с понедельника по пятницу**, может быть отменена до начала следующего рабочего дня (до 00:00) • внесенный **с 00:01 в субботу, воскресенье или в нерабочий день Банка**, может быть отменен до начала следующего рабочего дня (до 00:00)
• polecenie przelewu wewnętrznego, które wymaga przewalutowania	• внесенный **с 19:01 до 24:00 с понедельника по пятницу**, может быть отменена до начала следующего рабочего дня (до 00:00) • внесенный **с 00:01 в субботу, воскресенье или в нерабочий по закону день Банка**, может быть отменен до начала следующего рабочего дня (до 00:00)

Денежные средства в связи с отменой перевода будут возвращены на счет не позднее ближайшего рабочего дня.