

УТВЕРЖДЕНО
правлением АО «Датабанк»
(протокол заседания от 11.09.2019 года №16)
Действуют с 23.09.2019 г.

**Изменения № 1
к ПРАВИЛАМ УНИВЕРСАЛЬНОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ
ФИЗИЧЕСКИХ ЛИЦ В АО «ДАТАБАНК» (на публичных условиях) (УДБО)**

1. Дополнить Правила УДБО:

Приложением № 19 – Условия использования держателями карт АО «Датабанк» с применением платежного приложения Google Pay.

Приложение № 20 – Условия использования держателями карт АО «Датабанк» с применением платежного приложения Apple Pay.
следующего содержания:

Приложение №19
к Правилам универсального банковского обслуживания
физических лиц в АО «Датабанк»
(на публичных условиях) (УДБО)
Действуют с 23.09.2019 г.

**УСЛОВИЯ ИСПОЛЬЗОВАНИЯ ДЕРЖАТЕЛЯМИ КАРТ АО «ДАТАБАНК» С ПРИМЕНЕНИЕМ
ПЛАТЕЖНОГО ПРИЛОЖЕНИЯ GOOGLE PAY**

1. ТЕРМИНЫ

1.1. **Google Pay** – разработанная компанией Google Ireland Limited платежная платформа, которая обеспечивает возможность совершения транзакций Держателями карт Банка, зарегистрировавшими Карты в Google Pay. Поставщиком платежного приложения является Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA.

1.2. **NFC-карта** - электронное средство платежа, выпускаемое самостоятельно Держателем с использованием платежного приложения, установленного на Мобильном устройстве Держателя, к Карте, которое позволяет Держателю совершать операции по Счету Карты с использованием технологии беспроводной высокочастотной связи малого радиуса действия (NFC).

1.3. **Верификация Держателя карты** - процедура подтверждения полномочий (предоставление прав доступа) Держателя карты. При регистрации карты Верификация Держателя карты может осуществляться путем ввода Держателем карты Одноразового пароля, направленного на номер мобильного телефона, зафиксированный в информационных системах Банка. Время действия Одноразового пароля является ограниченным и определяется Банком. Применение Одноразового пароля является однократным. При совершении платежа Верификация Держателя карты осуществляется путем ввода Держателем карты Пароля или Отпечатка пальца и/или дополнительным вводом ПИН-кода карты (при платежах через POS-терминал).

1.4. **Верификация карты** – процедура дополнительной проверки Банком карты Держателя карты, осуществляемая с целью снижения рисков проведения мошеннической операции по карте. Верификация карты осуществляется по CVV2.

1.5. **Держатель карты** – физическое лицо, в том числе уполномоченное юридическим лицом/индивидуальным предпринимателем, на чье имя выпущена Карта.

1.6. **Мобильное приложение Банка (Ижкард.ру)** - установленное на Мобильном устройстве Apple приложение под маркой Банка, которое Держатели карт Банка применяют для управления Картами, счетами, иными продуктами Банка, а также их администрирования или использования с Мобильных устройств Apple.

1.7. **Мобильное устройство** – электронное устройство (мобильный телефон, смартфон, планшетный компьютер), находящееся в личном пользовании Держателя Карты, имеющее подключение к сети Интернет.

1.8. **Одноразовый пароль** – комбинация символов в виде цифр, генерируемая Банком при попытке зарегистрировать карту в платежном приложении и направляемая Держателю карты в виде Push-уведомления или СМС-сообщения на номер мобильного телефона Держателя карты, зафиксированный в информационных системах Банка.

1.9. **Отпечаток пальца** – однозначное цифровое представление персональных данных об особенностях строения папиллярных узоров пальца Держателя карты. Отпечаток пальца обеспечивает однозначную Верификацию Держателя карты.

1.10. **Пароль** – комбинация символов (цифр), служащая для Верификации Держателя карты в Мобильном устройстве. Пароль обеспечивает однозначную Верификацию Держателя карты в Мобильном устройстве. Пароль используется многократно и может быть изменен Держателем карты самостоятельно неограниченное количество раз.

1.11. **Персональные данные** – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных) – Держателю карты.

1.12. **ПИН-код карты** – персональный идентификационный номер (секретный код), выдаваемый Держателю Карты вместе с Картой в запечатанном конверте, известный только Держателю Карты, являющийся аналогом собственноручной подписи Держателя Карты, предназначенный для идентификации Держателя Карты при совершении операций с использованием Карты.

1.13. **Платежная система** – международная платежная система Visa International.

1.14. **Провайдер** – поставщик платежного сервиса Google Pay, позволяющего совершать платежи при помощи NFC-карты.

1.15. **Реквизиты NFC-карты** - номер и срок действия NFC-карты.

1.16. **Реквизиты карты** – информация, нанесенная на лицевую и/или оборотную сторону Карты, которая может включать в себя номер карты, срок действия Карты, данные владельца карты (при необходимости), трехзначное кодовое значение – CVV2, напечатанное на оборотной стороне Карты после последних четырех цифр ее номера. Реквизитами для виртуальной карты являются номер карты, срок действия карты, трехзначное кодовое значение – CVV2.

1.17. **Сайт Банка** – официальный сайт Банка в информационно-телекоммуникационной сети «Интернет» www.izhcombank.ru.

1.18. **Тарифы** – тарифы комиссионного вознаграждения, утвержденные Банком, действующие на дату оказания услуги (осуществления операции).

1.19. **Технология бесконтактных платежей** - технология бесконтактной оплаты с использованием Карты и/или Токена путем близкого поднесения (до 10 сантиметров) или прикосновения Мобильного устройства, с использованием которого создан Токен, или форм-фактором Карты (часы, телефон, брелоки и т.д.), к платёжному терминалу с технологией бесконтактных платежей.

1.20. **Токен (DPAN)** – цифровое представление карты, которое формируется по факту регистрации Карты и хранится в зашифрованном виде в защищенном хранилище Мобильного устройства и/или защищенном облачном хранилище Провайдера.

1.21. **Транзакция с удаленным доступом** - дистанционная платежная операция, совершаемая посредством Google Pay и запускаемая путем аутентификации пользователя на Мобильном устройстве без применения бесконтактного устройства в пункте продаж.

1.22. **Токенизация** – процесс создания Токена (DPAN) и его связки с Номером карты (FPAN), позволяющий однозначно определить Карту, использованную для совершения операций с использованием Google Pay.

1.23. **Условия** – настоящие Условия использования банковских карт АО «Датобанк» с применением платежного приложения Google Pay.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. По счетам, открытым в рамках Правил УДБО, Клиент вправе на основании и в соответствии с настоящими Условиями использовать платежное приложение Google Pay для совершения Транзакций с использованием Карты.

2.2. В соответствии с пунктом 3 статьи 438 Гражданского кодекса Российской Федерации присоединением Держателя карты к настоящим Условиям является совершение Держателем карты действий по подключению карты на Мобильном устройстве к Google Pay, после чего Мобильное устройство

может использоваться для совершения платежей с использованием Бесконтактных технологий, Транзакций с удаленным доступом.

2.3. Присоединение Держателя карты к настоящим Условиям означает, что Держатель карты:

- ознакомлен, согласен и принимает Условия;

- предоставляет право Банку самостоятельно проводить конвертацию списываемых денежных средств (при необходимости), при этом конвертация производится по текущему курсу Банка на момент списания. При разнице в курсах валют на момент Авторизации и момент списания, сумма, заблокированная в момент Авторизации, может отличаться от суммы реального списания;

- поручает Банку перечислять денежные средства со счета карты Держателя карты, которая подключена к Google Pay;

- ознакомлен с Тарифами Банка;

- дает согласие на получение от Банка, Платежного сервиса Google Pay SMS-сообщений/ Push-уведомлений, необходимых для совершения платежей с использованием Мобильного устройства;

- согласие на обработку своих персональных данных в соответствии с Правилами КБО и действующим законодательством.

2.4. Банк не является Провайдером в Google Pay и не предоставляет программное обеспечение, установленное на Мобильном устройстве, принадлежащем Держателю карты, в котором хранится Токен (DPAN).

2.5. Банк оказывает Держателю карты услуги по совершению Транзакций с использованием Карты посредством Google Pay в соответствии с настоящими Условиями до расторжения соответствующих договоров, регламентирующих взаимоотношения между Банком и Держателями карт.

2.6. Прекращение действия настоящих Условий не влияет на юридическую силу и действительность распоряжений, направленных в Банк Держателем карты до прекращения действия Условий.

2.7. Обслуживание Карты осуществляется в соответствии с заключенными между Банком и Клиентом Договором банковского счета с использованием Корпоративной банковской карты.

2.8. Банк не вправе предоставлять поставщику платежного приложения, указанному в п. 1.1. настоящих Условий, сведения об аналогах собственноручных подписей, кодах, паролях и иные сведения, используемые для удостоверения права Клиента распоряжаться денежными средствами.

2. ПОРЯДОК ВЫПУСКА И ИСПОЛЬЗОВАНИЯ NFC-КАРТЫ

3.1. Держатель может выпустить NFC-карту в порядке, определенном настоящим разделом.

3.2. Держателю предоставляется возможность выпуска NFC-карты только при наличии действующей Карты АО «Датабанк», выпущенной на имя Держателя.

3.3. NFC-карта не имеет физического носителя. Номер NFC-карты сохраняется в Мобильном устройстве Держателя. ПИН и срок действия NFC-карты такие же, как у Карты, к которой NFC-карта выпущена.

3.4. Выпуск NFC-карты возможен при наличии у Держателя доступа к сети Интернет через Мобильное устройство, которое поддерживает NFC-технологии, и соответствующего мобильного приложения.

3.5. Оформление NFC-карты осуществляется Держателем самостоятельно:

3.5.1. через соответствующее мобильное приложение на Мобильном устройстве путем ввода Реквизитов карты и ввода кода подтверждения, полученного Держателем в виде SMS-сообщения на номер мобильного телефона, подключенного к Карте. По факту выпуска NFC-карты Держателю направляется SMS-сообщение на номер мобильного телефона, подключенного к Карте. Совершение Держателем указанных выше действий, в том числе введения кода подтверждения, полученного Держателем в виде SMS-сообщения на номер мобильного телефона, подключенного к Карте, подтверждает ознакомление Держателя с Условиями выпуска и обслуживания NFC-карты, согласие с ними и присоединение к ним.

3.6. NFC-карта используется для совершения операций в ТСП, включая сеть Интернет.

3.7. Для улучшения качества обслуживания операций, совершаемых с использованием NFC-технологии и повышения безопасности оказываемых услуг, Банк оставляет за собой право изменять порядок и условия использования NFC-карты, известив об этом Держателя через Официальный сайт Банка.

3.8. Расчетные (расчетно-кассовые) документы, оформляемые при совершении операций с использованием NFC-карты, могут быть подписаны собственноручной подписью Держателя, либо с использованием аналога собственноручной подписи Держателя – ПИН-кода Карты, к которой выпущена

NFC-карта, либо путем прохождения аутентификации в соответствующем мобильном приложении, с использованием которого осуществлен выпуск NFC-карты на Мобильном устройстве (подтверждении биометрическими данными на Мобильном устройстве и/или ввода пароля Мобильного устройства, в памяти которого сохранены Реквизиты NFC-карты). Операции с использованием NFC-карты могут проводиться без ввода ПИН-кода или подписи Держателя на чеке. Расчетно-кассовые документы, подписанные или составленные указанными выше способами, являются надлежащим подтверждением того, что распоряжение на проведение операции по Счету Карты составлено и подписано Держателем.

3.9. В случае утраты Мобильного устройства, в памяти которого сохранены Реквизиты NFC-карты, Держатель должен незамедлительно сообщить об утрате Мобильного устройства/NFC-карты в Банк по телефонам Контактного Центра. Уведомление считается полученным в момент завершения телефонного разговора с оператором Контактного Центра Банка, в ходе которого Держатель предоставил всю необходимую информацию для выполнения блокировки NFC-карты.

3.10. Если пароль Мобильного устройства и/или Мобильное устройство, в памяти которого сохранены Реквизиты NFC-карты, стали доступны третьим лицам, Держатель должен немедленно сообщить об этом в Банк по телефонам Контактного Центра.

3.11. Для блокировки NFC-карты Держателю необходимо выполнить одно из следующих действий:

- обратиться в Контактный Центр Банка по телефонам Контактного Центра и следовать полученным инструкциям;

- удалить NFC-карту, используя соответствующее мобильное приложение, установленное на Мобильном устройстве Держателя.

Для дальнейшего использования NFC-карты, которая была заблокирована, Держателю необходимо обратиться в Банк.

Для дальнейшего использования NFC-карты, которая была удалена, Держателю необходимо оформить новую NFC-карту в соответствии с п.3.5.

3.12. В случае совершения операции с использованием NFC-карты без согласия Держателя, Держатель должен незамедлительно обратиться в Банк или в Контактный Центр Банка.

3.13. При перевыпуске Карты до истечения срока ее действия Банк осуществляет блокировку всех выпущенных к ней NFC-карт после подачи заявления в Банк в соответствии с договором банковского счета с использованием Корпоративной банковской карты. Для дальнейшего использования NFC-карты Держателю необходимо после получения выпущенной на новый срок Карты самостоятельно оформить NFC-карту в соответствии с п 3.5.

3.14. В случае отказа Банка в перевыпуске Карты в соответствии с Правилами КБО, все оформленные NFC-карты блокируются и их дальнейшее использование невозможно.

3.15. При отказе Держателя в соответствии с Правилами КБО от дальнейшего использования Карты, к которой выпущена NFC-карта, NFC-карта блокируется Банком и ее дальнейшее использование невозможно.

3.16. При установлении лимитов и ограничений в соответствии с Правилами КБО они также распространяются на NFC-карту.

3.17. При установлении Банком лимитов на проведение операций по Карте в соответствии с Правилами КБО они также распространяются на NFC-карту.

3.18. При совершении операций с использованием NFC-карты изменение расходного лимита Карты осуществляется в соответствии с Правилами КБО.

3.19. Информирование об операциях, совершенных с использованием NFC-карты, осуществляется в соответствии с порядком информирования об операциях, совершенных по Счету Карты, установленных Правилами КБО.

3.20. Держатель уполномочивает Банк:

3.20.1. передавать, в том числе на территорию иностранных государств (трансграничная передача), информацию о сумме операции, дате и времени ее совершения, типе операции, коде валюты, статусе авторизации для ее обработки Компанией Google Ireland Limited, являющейся владельцем платежного приложения Google Pay, обеспечивающей Держателям карт возможность совершать операции с использованием Карты посредством технологии беспроводной высокочастотной связи малого радиуса действия (NFC), и их аффилированным лицам, в целях:

- предоставления Держателям Карт в мобильном приложении информации о совершенных ими операциях по NFC-карте;

- обнаружения и устранения мошенничества;

- выполнения организациями - владельцами программного обеспечения (мобильных приложений) и их аффилированными лицами требований законодательства;
 - создания отчетов об экономической эффективности мобильных приложений исключительно для использования внутри организаций - владельцев программного обеспечения (мобильных приложений) и их аффилированных лиц;
 - рекламы мобильных приложений и иного их продвижения на рынке;
 - усовершенствования мобильных приложений;
 - проведения анализа распределения рекламных объявлений в мобильных приложениях;
- 3.20.2. передавать, в т.ч. на территорию иностранных государств (трансграничная передача), информацию о персональных данных Держателя (имя, адрес регистрации) компании Google Ireland Limited для выпуска NFC-карт путем прохождения регистрации Держателя в мобильном приложении Google Pay.

4. ТРЕБОВАНИЯ БЕЗОПАСНОСТИ

4.1. В целях безопасности Держатель карты обязуется:

- не оставлять Мобильное устройство без присмотра;
- обеспечить соответствующий уровень безопасности на Мобильном устройстве, используя Пароли и другие возможные методы блокировки/разблокировки Мобильного устройства;
- убедиться, что на Мобильном устройстве не зарегистрированы Отпечатки пальцев или иные способы разблокировки Мобильного устройства другого лица;
- не разглашать третьим лицам регистрационные данные от Мобильного устройства, если прекращено его использование;
- удалить все личные данные и финансовую информацию со старого Мобильного устройства, если прекращено его использование;
- обратиться в Контактный центр Банка как можно скорее, в случае подозрений на любое несанкционированное использование Мобильного устройства, а также, если Мобильное устройство был взломано, потеряно или украдено. Необходимо изменить учетные данные в Мобильном устройстве, чтобы избежать несанкционированного использования Карт;
- не блокировать любые функции безопасности, предусмотренные приложениями Мобильных устройств, для использования этих функций и процедур безопасности для защиты всех Карт;
- создать сложный Пароль;
- удалять информацию о Картах при передаче Мобильного устройства третьим лицам;
- не подвергать Мобильное устройство операциям повышения привилегий / взлома операционной системы устройства (rooting);
- в случае утери Мобильного устройства, Клиент/Держатель заблокировать (при возможности) платежное приложение Провайдера и/или удалить все данные из Платежного приложения с помощью функции удаленного поиска Мобильного устройства ("Найти мое Мобильное устройство") с целью предотвращения использования Платежного приложения третьими лицами;
- не сообщать реквизиты Карты третьим лицам для регистрации на Мобильных устройствах, не принадлежащих Клиенту/Держателю;
- не регистрировать Карту на Мобильных устройствах, принадлежащих третьим лицам.

5. ПРАВА И ОБЯЗАННОСТИ СТОРОН

5.1. Банк обязан:

- 5.1.1. исполнять распоряжения Держателя по операциям, совершенным с использованием реквизитов Карты, посредством Google Pay;
- 5.1.2. принять все возможные меры к недопущению приема распоряжений с использованием реквизитов Карты посредством Google Pay без предварительной успешной Верификации Держателя карты;
- 5.1.3. незамедлительно, но не позднее 30 (тридцати) минут с момента получения обращения Держателя карты об утрате Мобильного устройства, компрометации Карты (реквизитов Карты) и (или) утраты контроля над SIM-картой заблокировать Токены на данном Мобильном устройстве. При обращении Держателя карты по телефону блокировка Карты производится после идентификации Держателя карты по Кодовому слову. Блокировка Карты при обращении Держателя карты в офис Банка производится после предъявления документа, удостоверяющего личность, при получении от Держателя карты соответствующего письменного заявления;

5.1.4. в целях исполнения требований законодательства и обеспечения безопасности денежных средств Держателя карты, информировать Держателя карты о совершении каждой операции с использованием карты посредством Google Pay в соответствии с договором банковского счета с использованием Корпоративной банковской карты.

5.2. Банк имеет право:

5.2.1. Не исполнять распоряжения Держателя карты, совершенные с использованием Карты посредством Google Pay, в случаях:

- если Верификация Держателя / Верификация Карты произошла неуспешно;
- если Держателем карты не соблюдены требования законодательства Российской Федерации, настоящих Условий.

5.2.2. в целях обеспечения безопасности устанавливать ограничения по времени действия Одноразового пароля в пределах одного сеанса соединения;

5.2.3. запрашивать у Держателя карты информацию и документы в целях соблюдения требований действующего законодательства, в том числе Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», относительно характера и экономического смысла, предполагаемых или совершенных операций с использованием Реквизитов карты посредством Google Pay;

5.2.4. в любой момент потребовать от Держателя карты подписания документов на бумажном носителе, эквивалентных по смыслу и содержанию переданным Держателем карты и исполненным Банком распоряжений Держателя карты;

5.2.5. заблокировать, ограничить, приостановить или прекратить использование Реквизитов карты и платежей, совершенных с использованием Реквизитов карты посредством Google Pay, в случае, если Держатель карты нарушает настоящие Условия и/или действующее законодательство Российской Федерации, либо при наличии подозрений в совершении незаконных операций;

5.2.6. отказать Держателю карты в регистрации карты для совершения операций с использованием Реквизитов карты посредством Google Pay при неуспешной Верификации Держателя карты/ Верификации карты;

5.2.7. удалить Токен в случае неисполнения Держателем карты настоящих Условий.

5.3. Держатель карты обязан:

5.3.1. соблюдать положения настоящих Условий;

5.3.2. обеспечить конфиденциальность, а также хранение Мобильного устройства, Пароля, ПИН-кода карты, SIM-карты способом, исключая доступ к ним третьих лиц, а также немедленно уведомлять Банк о подозрении, что Мобильное устройство, Пароль, ПИН-код карты, SIM-карта могут быть использованы посторонними лицами;

5.3.3. в случае утраты Держателем карты мобильного устройства, Пароля, ПИН-кода карты, SIM-карты или наличия подозрений, что они используются третьими лицами, незамедлительно, после обнаружения указанных фактов, но не позднее дня, следующего за днем получения от Банка уведомления о совершенной операции, сообщить об этом Банку;

5.3.4. в течение 10 (десяти) календарных дней с момента изменения номера мобильного телефона Держателя карты, прекращения обслуживания номера мобильного телефона Держателя карты оператором сотовой связи или замены SIM-карты, сообщить об этом Банку. Банк, получив указанную информацию, имеет право приостановить предоставление Услуги до момента подтверждения принадлежности номера мобильного телефона Держателю карты путем обращения Держателя карты в Банк;

5.3.5. предоставлять информацию и документы, запрашиваемые Банком в целях соблюдения требований действующего законодательства, в том числе, Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» и Федерального закона от 28.06.2014 № 173-ФЗ «Об особенностях осуществления финансовых операций с иностранными гражданами и юридическими лицами, о внесении изменений в Кодекс Российской Федерации об административных правонарушениях и признании утратившими силу отдельных положений законодательных актов Российской Федерации», относительно характера и экономического смысла, предполагаемых или совершенных операций с использованием Реквизитов карты посредством Google Pay;

5.3.6. сохранять все документы, оформленные при совершении операций с использованием Реквизитов Карты посредством Google Pay, в течение 180 (ста восьмидесяти) календарных дней со дня

проведения каждой операции и предоставлять их по первому требованию в указанные Банком сроки для подтверждения правомерности совершения операции по Карте (Картам) или для урегулирования спорных вопросов/претензий;

5.3.7. оказывать содействие Банку при проведении любых расследований и использовать меры для предотвращения мошенничества, или иные меры, которые могут предотвратить компрометацию Реквизитов карты;

5.3.8. соблюдать требования безопасности, предусмотренные настоящими Условиями.

5.4. Держатель карты имеет право:

5.4.1. производить любые предусмотренные настоящими Условиями и не запрещенные действующим законодательством Российской Федерации операции посредством Google Pay;

5.4.2. предоставлять в офис Банка претензионное заявление по форме, установленной Банком, оформленное в письменном виде, в случае несогласия с операцией (-ями), совершенных с использованием Реквизитов карты посредством Google Pay, незамедлительно, но не позднее дня, следующего за днем получения от Банка уведомления о совершении операции. Неполучение Банком в течение указанного срока претензионного заявления свидетельствует о согласии Держателя карты с информацией об операциях, совершенных с использованием Реквизитов карты посредством Google Pay;

5.4.3. изменить способ уведомления о совершении операций с использованием Карты, оформив заявление на изменение способа уведомления (по форме Банка).

6. ОТВЕТСТВЕННОСТЬ СТОРОН

6.1. Клиент несет ответственность за:

- сохранение конфиденциальности идентификатора в системах Провайдера Токена (если применимо), Пароля и других средств Верификации Держателя;

- использование Мобильного устройства третьими лицами;

- за операции, совершенные Держателем в Google Pay с использованием реквизитов Карты, зарегистрированной на Мобильном устройстве Держателя;

- нарушение требований к технической защите Мобильного устройства, указанных в разделе 4 Условий, в том числе в случаях, когда Держатель использует Мобильное устройство, которое было подвергнуто операциям повышения привилегий / взлома операционной системы устройства (rooting);

- за операции, состоявшиеся в результате невыполнения обязанностей, предусмотренных настоящими Условиями.

6.2. Ответственность Банка.

6.2.1. Банк не несет ответственности:

• за работу Google Pay, ее функционирование и взаимосвязь с другими приложениями, установленными на Мобильном устройстве;

• за отсутствие возможности совершения посредством Google Pay операций;

• за любую блокировку, приостановление, аннулирование или прекращение использования Карты в Google Pay;

• за какие-либо убытки или ущерб, понесенные Держателем карты в связи с утерей, кражей или порчей Мобильного устройства;

• Банк не несет ответственности за поддержку операционной системы Мобильного устройства.

6.2.2. Банк несет ответственность за исполнение Условий в соответствии с действующим законодательством Российской Федерации.

УСЛОВИЯ ИСПОЛЬЗОВАНИЯ БАНКОВСКИХ КАРТ АО «ДАТАБАНК» С ПРИМЕНЕНИЕМ ПЛАТЕЖНОГО ПРИЛОЖЕНИЯ APPLE PAY

1. ИСПОЛЬЗУЕМЫЕ ТЕРМИНЫ

1.1. **Apple ID** – уникальный идентификатор Держателя карты как пользователя Мобильного устройства Apple, присваиваемый Корпорацией Apple.

1.2. **Apple Pay** – платежная платформа, использующая технологии Корпорации Apple в целях предоставления пользователям возможности осуществлять платежи при помощи Карт и других материальных, цифровых или виртуальных платежных карт, параметров доступа или устройств доступа к счету, а также получать доступ к другим сопутствующим услугам с использованием Продукции Корпорации Apple, указанной Корпорацией Apple или аффилированными лицами Корпорации Apple. Поставщиком платежного приложения является Apple Distribution International Hollyhill Industrial Estate, Cork, Ireland.

1.3. **Apple Wallet** – предустановленная на Мобильном устройстве Apple программа, позволяющая осуществить Токенизацию и хранить информацию о Токенах, а также информацию, позволяющую однозначно различить ту или иную карту: изображение карты, последние 4 цифры Номера карты (FPAN).

1.4. **iCloud** – интернет-сервис Корпорации Apple. Доступ в iCloud осуществляется посредством приложения «Настройки» на Мобильном устройстве Apple и ввода Держателем карты своего Apple ID.

1.5. **Push-уведомления** – краткие уведомления, всплывающие на экране Мобильного устройства Apple. Push-уведомления могут поступать исключительно при наличии доступа к сети интернет.

1.6. **Touch ID** – дактилоскопический датчик/сканер Отпечатков пальцев, разработанный Корпорацией Apple и предустановленный в Мобильных устройствах Apple. Touch ID позволяет Держателям карт, в том числе, использовать Отпечаток пальца в качестве подтверждения покупки в App Store, iTunes Store и iBooks Store.

1.7. **Верификация Держателя карты** - процедура подтверждения полномочий (предоставление прав доступа) Держателя карты. При регистрации карты в Apple Wallet, Верификация Держателя карты может осуществляться путем ввода Держателем карты Одноразового пароля, направленного на номер мобильного телефона, зафиксированный в информационных системах Банка. Время действия Одноразового пароля является ограниченным и определяется Банком. Применение Одноразового пароля является однократным. При совершении платежа Верификация Держателя карты осуществляется путем ввода Держателем карты Пароля или Отпечатка пальца и/или дополнительным вводом ПИН-кода карты (при платежах через POS-терминал).

1.8. **Верификация карты** – процедура дополнительной проверки Банком карты Держателя карты, осуществляемая с целью снижения рисков проведения мошеннической операции по карте. Верификация карты осуществляется по CVV2 коду.

1.9. **Держатель карты** – физическое лицо, в том числе уполномоченное юридическим лицом/индивидуальным предпринимателем, на чье имя выпущена Карта.

1.10. **Кодовое слово** – секретный пароль, назначаемый Держателем карты самостоятельно, не подлежащий разглашению третьим лицам, предназначенный для подтверждения личности Держателя карты в случаях, предусмотренных Универсальным договором банковского обслуживания (далее - УДБО). Кодовое слово может устанавливаться и изменяться Держателем карты необходимое количество раз на основании письменного заявления Держателя карты.

1.11. **Корпорация Apple** - ЭППЛ ДИСТРИБЬЮШН ИНТЕРНЭШНЛ (Apple Distribution International) - ирландская корпорация с неограниченной ответственностью, с местонахождением основного коммерческого предприятия по адресу: Промышленная зона Холли Хилл, Корк, Ирландия [Holly Hill Industrial Estate, Cork, Ireland].

1.12. **Мобильное устройство Apple** - электронное устройство корпорации Apple (мобильный телефон, смартфон, планшетный компьютер), находящееся в личном пользовании Держателя Карты, имеющее подключение к сети Интернет. По настоящим Условиям под данную категорию устройств

подпадают мобильные телефоны iPhone: iPhone 6, 6 Plus, iPhone 6S, 6S Plus, 7, 7 Plus, iPhone SE; iPad: iPad Air 2, iPad Pro, Apple Watch и более поздние версии этих устройств.

1.13. **Мобильное приложение Банка (Ижкард.ру)** - установленное на Мобильном устройстве Apple приложение под маркой Банка, которое Держатели карт Банка применяют для управления Картами, счетами, иными продуктами Банка, а также их администрирования или использования с Мобильных устройств Apple.

1.14. **Номер карты (FPAN)** – уникальный набор цифр, наносимый эмбоссером (иным устройством персонализации) на лицевую сторону Карты. Номер карты состоит из шестнадцати цифр.

1.15. **Одноразовый пароль** – комбинация символов в виде цифр, генерируемая Банком при попытке зарегистрировать карту в Apple Wallet и направляемая Держателю карты в виде Push уведомления или СМС сообщения на номер мобильного телефона Держателя карты, зафиксированный в информационных системах Банка.

1.16. **Отпечаток пальца** – однозначное цифровое представление персональных данных об особенностях строения папиллярных узоров пальца Держателя карты. Отпечаток пальца обеспечивает однозначную Верификацию Держателя карты.

1.17. **Пароль** – комбинация символов (цифр), служащая для Верификации Держателя карты в Мобильном устройстве Apple. Пароль обеспечивает однозначную Верификацию Держателя карты в Мобильном устройстве Apple. Пароль используется многократно и может быть изменен Держателем карты самостоятельно неограниченное количество раз.

1.18. **Персональные данные** – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных) – Держателю карты.

1.19. **ПИН-код карты** – персональный идентификационный номер (секретный код), выдаваемый Держателю Карты вместе с Картой в запечатанном конверте, известный только Держателю Карты, являющийся аналогом собственноручной подписи Держателя Карты, предназначенный для идентификации Держателя Карты при совершении операций с использованием Карты.

1.20. **Платежная система** – платежная система Visa International.

1.21. **Провайдер** – поставщик платежного сервиса Apple Pay, позволяющего совершать платежи при помощи iPhone и Apple Watch.

1.22. **Реквизиты карты** – информация, нанесенная на лицевую и/или оборотную сторону Карты, которая может включать в себя номер карты, срок действия Карты, данные владельца карты (при необходимости), трехзначное кодовое значение - CVV2, напечатанное на оборотной стороне Карты после последних четырех цифр ее номера. Реквизитами для виртуальной карты являются номер карты, срок действия карты, трехзначное кодовое значение - CVV2.

1.23. **Сайт Банка** – официальный сайт Банка в информационно-телекоммуникационной сети «Интернет» www.izhcombank.ru.

1.24. **Тарифы** – тарифы комиссионного вознаграждения, утвержденные Банком, действующие на дату оказания услуги (осуществления операции).

1.25. **Технология бесконтактных платежей** - технология бесконтактной оплаты с использованием Карты и/или Токена путем близкого поднесения (до 10 сантиметров) или прикосновения Мобильного устройства, с использованием которого создан Токен, или форм-фактором Карты (часы, телефон, брелоки и т.д.), к платёжному терминалу с технологией бесконтактных платежей.

1.26. **Токен (DPAN)** – цифровое представление карты, которое формируется по факту регистрации Карты в Apple Wallet и хранится в зашифрованном виде в защищенном хранилище Мобильного устройства Apple.

1.27. **Транзакция с удаленным доступом** - дистанционная платежная операция, совершаемая посредством Apple Pay и запускаемая путем аутентификации пользователя на Мобильном устройстве Apple без применения бесконтактного устройства в пункте продаж.

1.28. **Токенизация** – процесс создания Токена (DPAN) и его связки с Номером карты (FPAN), позволяющий однозначно определить Карту, использованную для совершения операций с использованием Apple Pay. Токенизация осуществляется по факту добавления Карты в Apple Wallet.

1.29. **Условия** – настоящие Условия использования банковских карт АО «Датабанк» с применением платежного приложения Apple Pay.

1.30. **Услуга** – услуга по проведению операций с использованием Реквизитов карты посредством Apple Pay, в том числе операций с применением Бесконтактной технологии и Транзакций с удаленным доступом.

2. ПРЕДЛОЖЕНИЕ БАНКА И ПОРЯДОК ЕГО ПРИНЯТИЯ ДЕРЖАТЕЛЕМ КАРТЫ

2.1. По счетам, открытым в рамках Правил УДБО, Клиент вправе на основании и в соответствии с настоящими Условиями использовать платежное приложение Apple Pay для совершения Транзакций с использованием Карты.

2.2. В соответствии с пунктом 3 статьи 438 Гражданского кодекса Российской Федерации присоединением Держателя карты к настоящим Условиям является совершение Держателем карты действий по подключению карты на Мобильном устройстве Apple к Apple Pay, после чего Мобильное устройство Apple может использоваться для совершения платежей с использованием Бесконтактных технологий, Транзакций с удаленным доступом.

2.3. Присоединение Держателя карты к настоящим Условиям означает, что Держатель карты:

- ознакомлен, согласен и принимает Условия;
- предоставляет право Банку самостоятельно проводить конвертацию списываемых денежных средств (при необходимости), при этом конвертация производится по текущему курсу Банка на момент списания. При разнице в курсах валют на момент Авторизации и момент списания, сумма, заблокированная в момент Авторизации, может отличаться от суммы реального списания;
- поручает Банку перечислять денежные средства со счета карты Держателя карты, которая подключена к Apple Pay;
- ознакомлен с Тарифами Банка;
- дает согласие на получение от Банка, Корпорации Apple (системы Apple Pay) SMS сообщений/ Push-уведомлений, необходимых для совершения платежей с использованием Мобильного устройства Apple;
- согласие на обработку своих персональных данных, в том числе на любые действия с персональными данными, включая их сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (включая распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение; в отношении любой относящейся к Держателю карты информации, полученной Банком, как от Держателя карты, так и от третьих лиц на срок действия настоящих Условий; на обработку персональных данных любым способом, в том числе с использованием средств автоматизации (включая программное обеспечение), так и без использования средств автоматизации (с использованием различных материальных носителей, включая бумажные носители), как Банку, так и его агентам, партнерам. Помимо прочего вышеуказанное согласие распространяется на передачу Банком Платежной системе персональных данных Держателя карты в соответствии с настоящими Условиями, в том числе, но не ограничиваясь, следующих данных: номер мобильного телефона, адрес электронной почты, Реквизиты карты; получение (сбор) Банком (как с использованием средств автоматизации, так и без использования средств автоматизации) от Платежной системы персональных данных Держателя карты, а также на иную обработку Банком таких персональных данных, полученных от Платежной системы, включая передачу. Настоящее согласие предоставляется на срок оказания Банком Держателю карты Услуги. Действие согласия пролонгируется на следующие пять лет после прекращения оказания Банком Держателю карты Услуги при отсутствии сведений о его отзыве. Настоящее согласие дается Держателем карты в целях осуществления платежей посредством использования Apple Pay и исполнения настоящих Условий в целом. Держатель карты подтверждает, что Банк осуществляет обработку персональных данных Держателя карты в течение всего срока действия согласия, если иное не предусмотрено действующим законодательством Российской Федерации;
- согласие на обработку персональных данных с целью их передачи уполномоченным государственным органам Российской Федерации, а также с целью трансграничной передачи иностранному налоговому органу, включая Internal Revenue Service of the United States (Федеральную налоговую службу США) и (или) иностранным налоговым агентам, уполномоченным иностранным налоговым органом на удержание иностранных налогов и сборов на условиях, в порядке и объеме, определенных законодательством Российской Федерации.

3. ОБЩИЕ ПОЛОЖЕНИЯ

3.1. Предметом настоящих Условий являются действия Банка, связанные с использованием карт Держателями карт в соответствии с Договором банковского счета с использованием Корпоративной банковской карты, настоящими Условиями и осуществлением Держателями карт с помощью Мобильных устройств Apple посредством Apple Pay платежей с применением Бесконтактной технологии, а также совершением Транзакций с удаленным доступом.

Взаимоотношения между Банком, Корпорацией Apple и иными лицами, привлекаемыми ими, не урегулированные Условиями, в которых не участвует Держатель карты, регламентируются отдельными договорами и/или соглашениями между ними и/или действующим применимым правом соответствующего государства.

3.2. Банк не является Провайдером в Apple Pay и не предоставляет программное обеспечение (приложение Apple Wallet), установленное на Мобильном устройстве Apple, принадлежащее Держателю карты, в котором хранится Токен (DPAN).

3.3. Банк оказывает Держателю карты Услугу в соответствии с настоящими Условиями до расторжения соответствующих договоров, регламентирующих взаимоотношения между Банком и Держателями карт.

3.5. Прекращение действия настоящих Условий не влияет на юридическую силу и действительность распоряжений, направленных в Банк Держателем карты до прекращения действия Условий.

3.6. Обслуживание Карты осуществляется в соответствии с заключенными между Банком и Клиентом Договором банковского счета с использованием Корпоративной банковской карты.

3.7. Банк не вправе предоставлять поставщику платежного приложения, указанному в п. 1.2. настоящих Условий, сведения об аналогах собственноручных подписей, кодах, паролях и иные сведения, используемые для удостоверения права Клиента распоряжаться денежными средствами.

4. ПОРЯДОК ПОДКЛЮЧЕНИЯ КАРТ

4.1. Для настройки Apple Pay должен быть совершен вход в учетную запись iCloud.

4.2. Для осуществления подключения Apple Pay потребуется подключение к интернету.

4.3. Для подключения Apple Pay необходимо добавить карту в приложение Apple Wallet на Мобильном устройстве Apple.

4.4. Порядок подключения к Apple Pay:

4.4.1. С помощью Мобильного приложения Банка («Ижкард.ру») iPhone, iPad:

- Открыть Мобильное приложение Банка («Ижкард.ру»).
- На поле страницы необходимо выбрать карту, которую необходимо подключить к Apple Pay.
- Нажать кнопку «Добавить в Apple Wallet».
- Следуя подсказкам системы, добавить карту в Apple Wallet на iPhone и ввести Реквизиты карты, которые запрашивает система (Верификация карты).
- После введения необходимых сведений следует ознакомиться с настоящими Условиями и принять их.

- Следовать дальнейшим информационным сообщениям системы.

При добавлении карты через Мобильное приложение Банка («Ижкард.ру») не требуется Верификация Держателя карты.

4.4.2. С помощью Apple Wallet:

- Открыть приложение Apple Wallet.
- Выбрать кнопку «+» или «Добавить Карту».
- Следуя подсказкам системы, ввести Реквизиты карты вручную или с использованием камеры Мобильного устройства Apple (Верификация карты).
- После введения необходимых сведений следует ознакомиться с настоящими Условиями и принять их.

- Для окончания процедуры подключения потребуется ввести Одноразовый пароль (Верификация Держателя карты) и следовать дальнейшим информационным сообщениям системы.

4.4.3. На устройствах Apple Watch:

- Открыть приложение Apple Watch на iPhone.
- Следуя подсказкам системы ввести Реквизиты карты, которые запрашивает система (Верификация карты).

- После введения необходимых сведений следует ознакомиться с настоящими Условиями и принять их.

- Для окончания процедуры подключения потребуется ввести Одноразовый пароль (Верификация Держателя карты) и следовать дальнейшим информационным сообщениям системы.

4.5. После успешной Верификации карты/Держателя карты и успешного добавления карты в Apple Wallet в защищенном хранилище Мобильного устройства Apple формируется и хранится Токен. Токен позволяет однозначно идентифицировать карту, используемую при совершении платежей посредством Apple Pay. По факту успешной регистрации карты в Apple Wallet, система Apple Pay/Банк направляет Держателю карты соответствующее Push уведомление/SMS-сообщение.

4.6. Удаление подключенной к Apple Pay карты осуществляется посредством выбора соответствующей кнопки «Удалить карту» на Мобильном устройстве Apple, с использованием которого происходило подключение.

4.7. После завершения подключения карты к Apple Pay Держатель карты может воспользоваться Услугой, предоставляемой в соответствии с настоящими Условиями:

- осуществлять платежи через POS терминал, установленный в ТСП, оснащенный технологией бесконтактной связи;

- осуществлять платежи в мобильных приложениях на Мобильном устройстве Apple, поддерживающих расчеты посредством Apple Pay (Транзакции с удаленным доступом).

Если платеж совершен через POS терминал, то подтверждение платежа может осуществляться с использованием Touch ID на Мобильном устройстве Apple, вводом Пин-кода карты при совершении операций на определенную сумму.

4.8. Держатель карты, осуществляя платеж посредством Apple Pay, регистрацию карты в Apple Wallet, используя при этом Одноразовый пароль/Отпечаток пальца, подтверждает возникновение и использование им аналога собственноручной подписи. Держатель карты признает, что электронный документ, сформированный для осуществления платежа посредством Apple Pay с аналогом собственноручной подписи, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью.

5. ПРАВА И ОБЯЗАННОСТИ СТОРОН

5.1. Банк обязан:

5.1.1. исполнять распоряжения Держателя карты по операциям, совершенным с использованием Реквизитов карты посредством Apple Pay;

5.1.2. принять все возможные меры к недопущению приема распоряжений с использованием Реквизитов карты в Apple Wallet, Apple Pay без предварительной успешной Верификации Держателя карты/Верификации карты, в случаях, когда такая верификация необходима;

5.1.3. незамедлительно, но не позднее 30 (тридцати) минут с момента получения обращения Держателя карты об утрате Мобильного устройства Apple, компрометации Реквизитов карты и (или) утраты контроля над SIM-картой, заблокировать Токены на данном Мобильном устройстве Apple. При обращении Держателя карты по телефону блокировка карты производится после идентификации Держателя карты по Кодовому слову. Блокировка карты при обращении Держателя карты в офис Банка производится после предъявления документа, удостоверяющего личность, при получении от Держателя карты соответствующего письменного заявления;

5.1.4. в целях исполнения требований законодательства и обеспечения безопасности денежных средств Держателя карты, информировать Держателя карты о совершении каждой операции с использованием карты посредством Apple Pay в соответствии с договором банковского счета с использованием Корпоративной банковской карты.

5.2. Банк имеет право:

5.2.1. не исполнять распоряжения Держателя карты, совершенные с использованием карты посредством Apple Pay, в случаях:

- если Верификация Держателя карты/ Верификация карты произошла неуспешно;

- если Держателем карты не соблюдены требования законодательства Российской Федерации, настоящих Условий;

5.2.2. в целях обеспечения безопасности устанавливать ограничения по времени действия Одноразового пароля в пределах одного сеанса соединения;

5.2.3. запрашивать у Держателя карты информацию и документы в целях соблюдения требований действующего законодательства, в том числе Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», относительно характера и экономического смысла, предполагаемых или совершенных операций с использованием Реквизитов карты посредством Apple Pay;

5.2.4. в любой момент потребовать от Держателя карты подписания документов на бумажном носителе, эквивалентных по смыслу и содержанию переданным Держателем карты и исполненным Банком распоряжений Держателя карты;

5.2.5. заблокировать, ограничить, приостановить или прекратить использование Реквизитов карты в Apple Wallet и платежей, совершенных с использованием Реквизитов карты посредством Apple Pay, в случае, если Держатель карты нарушает настоящие Условия и/или действующее законодательство Российской Федерации, либо при наличии подозрений в совершении незаконных операций;

5.2.6. отказать Держателю карты в регистрации карты в Apple Wallet для совершения операций с использованием Реквизитов карты посредством Apple Pay при неуспешной Верификации Держателя карты/Верификации карты;

5.2.7. удалить Токен в случае неисполнения Держателем карты настоящих Условий.

5.3. Держатель карты обязан:

5.3.1. соблюдать положения настоящих Условий;

5.3.2. обеспечить конфиденциальность, а также хранение Мобильного устройства Apple, Пароля, Пин-кода карты, SIM карты способом, исключающим доступ к ним третьих лиц, а также немедленно уведомлять Банк о подозрении, что Мобильное устройство Apple, Пароль, Пин-код карты, SIM карта могут быть использованы посторонними лицами;

5.3.3. в случае утраты Держателем карты мобильного устройства Apple, Пароля, Пин-кода карты, SIM карты или наличия подозрений, что они используются третьими лицами, незамедлительно, после обнаружения указанных фактов, но не позднее дня, следующего за днем получения от Банка уведомления о совершенной операции, сообщить об этом Банку;

5.3.4. в течение 10 (десяти) календарных дней с момента изменения номера мобильного телефона Держателя карты, прекращения обслуживания номера мобильного телефона Держателя карты оператором сотовой связи или замены SIM карты, сообщить об этом Банку. Банк, получив указанную информацию, имеет право приостановить предоставление Услуги до момента подтверждения принадлежности номера мобильного телефона Держателю карты путем обращения Держателя карты в Банк;

5.3.5. предоставлять информацию и документы, запрашиваемые Банком в целях соблюдения требований действующего законодательства, в том числе, Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» и Федерального закона от 28.06.2014 № 173-ФЗ «Об особенностях осуществления финансовых операций с иностранными гражданами и юридическими лицами, о внесении изменений в Кодекс Российской Федерации об административных правонарушениях и признании утратившими силу отдельных положений законодательных актов Российской Федерации», относительно характера и экономического смысла, предполагаемых или совершенных операций с использованием Реквизитов карты посредством Apple Pay;

5.3.6. сохранять все документы, оформленные при совершении операций с использованием Реквизитов Карты посредством Apple Pay, в течение 180 (ста восьмидесяти) календарных дней со дня проведения каждой операции и предоставлять их по первому требованию в указанные Банком сроки для подтверждения правомерности совершения операции по Карте (Картам) или для урегулирования спорных вопросов/претензий;

5.3.7. оказывать содействие Банку при проведении любых расследований и использовать меры для предотвращения мошенничества, или иные меры, которые могут предотвратить компрометацию Реквизитов карты;

5.3.8. исключить доступ третьих лиц к Apple Pay на Мобильном устройстве Apple;

5.3.9. обеспечить соответствующий уровень безопасности на Мобильном устройстве Apple, используя Пароли, Touch ID и другие возможные методы блокировки/разблокировки Мобильного устройства Apple;

5.3.10. убедиться, что на Мобильном устройстве Apple не зарегистрированы Отпечатки пальцев другого лица;

5.3.11. не разглашать третьим лицам регистрационные данные от Мобильного устройства Apple, такие как Apple ID, Пароль;

5.3.12. удалить все личные (персональные) данные и финансовую информацию с Мобильного устройства Apple, если прекращено его использование;

5.3.13. незамедлительно обратиться в Банк в случае подозрений на любое несанкционированное использование Мобильного устройства Apple, а также, если Мобильное устройство Apple было взломано, потеряно или украдено;

5.3.14. не блокировать любые функции безопасности, предусмотренные приложениями Мобильного устройства Apple, для использования этих функций и процедур безопасности для защиты всех карт, зарегистрированных в Apple Wallet;

5.3.15. удалять информацию о картах в Apple Wallet при передаче Мобильного устройства Apple третьим лицам;

5.3.16. не подвергать Мобильное устройство Apple операциям повышения привилегий/ взлома операционной системы устройства;

5.3.17. незамедлительно обратиться в Банк при получении SMS-сообщения о регистрации карты в Apple Wallet, если Держатель карты не осуществлял такой регистрации;

5.3.18. не использовать реквизиты карты в Apple Wallet и не совершать/пытаться совершить операции с использованием Реквизитов карты посредством Apple Pay до активации карты, а также после прекращения действия карты и в случаях блокирования такой карты.

5.4. Держатель карты имеет право:

5.4.1. производить любые предусмотренные настоящими Условиями и не запрещенные действующим законодательством Российской Федерации операции посредством Apple Pay;

5.4.2. предоставлять в офис Банка претензионное заявление по форме, установленной Банком, оформленное в письменном виде, в случае несогласия с операцией (-ями), совершенных с использованием Реквизитов карты посредством Apple Pay, незамедлительно, но не позднее дня, следующего за днем получения от Банка уведомления о совершении операции. Неполучение Банком в течение указанного срока претензионного заявления свидетельствует о согласии Держателя карты с информацией об операциях, совершенных с использованием Реквизитов карты посредством Apple Pay;

5.4.3. изменить способ уведомления о совершении операций с использованием карты, оформив заявление на изменение способа уведомления (по форме Банка).

6. ОТВЕТСТВЕННОСТЬ СТОРОН

6.1. Держатель карты несет ответственность перед Банком за:

- сохранение конфиденциальности Apple ID, Пароля и других средств Верификации Держателя карты;
- использование Мобильного устройства Apple третьими лицами;
- за операции, совершенные Держателем карты посредством Apple Pay с использованием Реквизитов карты, зарегистрированной в Apple Wallet на Мобильном устройстве Apple Держателя карты;
- нарушение предусмотренных настоящими Условиями обязанностей Держателя карты по обеспечению технической защиты Мобильного устройства Apple, указанных в разделе 5 настоящих Условий, в том числе в случаях, когда Держатель карты использует Мобильное устройство Apple Pay, которое было подвергнуто операциям повышения привилегий/ взлома операционной системы устройства.

6.2. Банк несет ответственность перед Держателем за:

- сохранность денежных средств Держателя карты при условии соблюдения Держателем карты настоящих Условий, УДБО и Тарифов;
- неисполнение своих обязательств в соответствии с действующим законодательством РФ (ст. 856 и ст. 866 Гражданского кодекса РФ).

6.3. Банк не несет ответственности:

- за работу Apple Pay,
- за отсутствие возможности совершения операций посредством Apple Pay,
- за любое блокирование, приостановление, аннулирование или прекращение использования карты посредством Apple Pay,
- за конфиденциальность информации, хранящейся на Мобильном устройстве Apple, в том числе в Apple Wallet;
- за поддержку операционной системы (iOS) Мобильного устройства Apple;

- за действия Провайдера или любой другой третьей стороны, совершаемые в рамках обслуживания Apple Wallet, Apple Pay;
- за любые обстоятельства, которые могут прервать, помешать или иным образом повлиять на функционирование Apple Wallet, Apple Pay, такие как недоступность сети оператора мобильной связи, а также ограничения зоны покрытия сети мобильной связи, перебои в подаче или прерывание беспроводного соединения.

7. ПРОЧИЕ ПОЛОЖЕНИЯ

7.1. Все споры, возникающие в связи с оказанием Услуги, а также споры, возникающие из публичной оферты или в связи с ней, подлежат разрешению в суде в соответствии с действующим законодательством Российской Федерации.

7.2. Срок для принятия (акцепта) публичной оферты не установлен.

7.3. Банк вправе отозвать публичную оферту. При этом уведомление об отзыве публичной оферты осуществляется одним из следующих способов (по выбору Банка):

- путем размещения информации об отзыве публичной оферты на информационных стендах по месту нахождения Банка и его подразделений;

- путем размещения информации об отзыве публичной оферты на Сайте Банка.

7.4. Настоящим Держатель карты уведомлен, понимает и соглашается с тем, что:

- не все юридические лица и индивидуальные предприниматели, осуществляющие реализацию товаров, выполнение работ, оказание услуг, а также не все кредитные организации могут обеспечить возможность приема Реквизитов карты для совершения операции оплаты посредством Apple Pay;

- платежные системы и/или другие кредитные организации могут вводить ограничения, в том числе по суммам операций с использованием Реквизитов карты посредством Apple Pay, а также устанавливать свои комиссии в отношении таких операций;

- совершение операций с использованием Реквизитов карты посредством Apple Pay может быть ограничено функциональностью программного обеспечения Мобильного устройства Apple, в том числе Apple Wallet;

- доступ, использование и возможность совершения операций с использованием Реквизитов карты посредством Apple Pay зависит исключительно от Apple Pay, от состояния сетей беспроводной связи, используемой Провайдером;

- Банк не контролирует и не влияет на обслуживание беспроводных сетей связи, на систему отключения / прерывания беспроводного соединения;

- Банк не гарантирует конфиденциальность и безопасность передачи данных в связи с электронной передачей данных через сторонние подключения, не попадающие под контроль Банка. Обеспечение конфиденциальности и безопасности передачи данных осуществляется в соответствии с регламентами Корпорации Apple;

- по любым вопросам, связанным с технической поддержкой Мобильного устройства Apple, о минимальных требованиях к программному и аппаратному обеспечению Держатель карты должен обращаться напрямую к Провайдеру;

- порядок получения и обработки любой информации, получаемой Провайдером в процессе использования Держателем карты Apple Pay, регулируется договором между Держателем карты и Провайдером;

- Провайдер, оператор мобильной связи, а также иные третьи лица, задействованные в предоставлении Услуги, имеют свои условия обслуживания и политики конфиденциальности. Передавая указанным лицам свои личные данные, используя услуги или посещая сайты в сети интернет указанных лиц, Держатель карты принимает их условия обслуживания и политики конфиденциальности.

7.5. Настоящим Банк уведомляет Держателя карты о повышенном риске использования Реквизитов карты при пользовании Услугой, в том числе при утрате Мобильного устройства Apple с установленным на нем Apple Wallet, в память которого внесены Реквизиты карты, компрометации Реквизитов карты. При утрате Мобильного устройства Apple, компрометации Реквизитов карты, доступ к возможности использования Реквизитов карты может получить третье лицо. Поэтому для снижения рисков Держатель карты должен в полной мере исполнять требования настоящих Условий, в том числе предпринимать все разумные и достаточно необходимые меры по безопасности и защите Мобильного устройства Apple с

установленным на нем Apple Wallet, в память которого записаны Реквизиты карты, а также информации и документов, обмен которыми производится в рамках Договора банковского счета/Договора по обслуживанию банковских карт, настоящих Условий.

2. Настоящие Изменения вступают в силу с 23.09.2019г.