Условия
использования расчетных карт АКБ «ТЕНДЕР-БАНК» (АО)
в Системе Apple Pay

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Apple ID – уникальный идентификатор Клиента как пользователя Мобильного устройства Apple, присваиваемый Apple Inc.

Авторизация платежа - процедура получения подтверждения Банком на проведение операции с использованием Карты посредством информационного обмена между участниками расчетов.

Банк – АКБ «ТЕНДЕР-БАНК» (АО). Банк осуществляет выпуск Карт, и обязуется обеспечивать расчеты по операциям, совершенным Клиентами с использованием Карт в Системе Apple Pay.

Верификация Карты - процедура дополнительной проверки Банком Карты Клиента, осуществляемая с целью снижения рисков проведения мошеннической операции по Карте Клиента. Верификация Карты осуществляется по Технологии CVC2/CVV2 кода.

Верификация Клиента - процедура подтверждения полномочий (предоставление прав доступа) Клиента.

При регистрации Карты в Apple Wallet, Верификация Клиента может осуществляться путем ввода Клиентом 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 Клиента осуществляется путем ввода Клиентом Пароля или Отпечатка пальца и/или дополнительным вводом ПИН-кода Карты (при платежах через POS-терминал).

Банк-Клиент для частных лиц – используемые Банком организационно-технические системы дистанционного банковского обслуживания физических лиц, при котором доступ к счетам Клиентов Банка, в том числе для совершения операций по ним, предоставляется в любое время и с любого компьютера (иного устройства), имеющего доступ в интернет. Обслуживание Клиента Банка посредством Банк-Клиента для частных лиц осуществляется в соответствии с Условиями дистанционного банковского обслуживания физических лиц в АКБ «ТЕНДЕР-БАНК» (АО) с использованием Системы ДБО «ТЕНДЕР-БАНК-Онлайн» (в действующей редакции).

Карта – международная банковская карта Платежной системы MasterCard WorldWide, выпускаемая Банком в качестве средства для составления расчетных и иных документов, подлежащих оплате, осуществления операций по СКС и получения информации о СКС.

Клиент – физическое лицо, являющееся держателем Карты, и имеющее Мобильное устройство Apple.

Мобильное устройство Apple – устройство (смартфон, планшет, часы) выпускаемое корпорацией Apple Inc. с поддержкой Системы Apple Pay (список указан на сайте www.apple.com/apple-pay/).

Мобильный Банк – используемая Банком организационно-техническая система дистанционного банковского обслуживания физических лиц, при котором доступ к счетам Клиентов, в том числе для совершения операций по ним, предоставляется в любое время с мобильного устройства, имеющего доступ в интернет. Обслуживание Клиента Банка посредством Мобильного Банка осуществляется в соответствии с Условиями дистанционного банковского обслуживания физических лиц в АКБ «ТЕНДЕР-БАНК» (АО) с использованием Системы ДБО «ТЕНДЕР-БАНК-Онлайн» (в действующей редакции).

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

Одноразовый пароль – комбинация символов в виде 6-ти цифр, генерируемая Банком при попытке зарегистрировать Карту в Apple Wallet, и направляемая Клиенту в виде Push-уведомления или СМС-сообщения на номер мобильного телефона Клиента, зафиксированный в информационных системах Банка.

Отпечаток пальца – однозначное цифровое представление рисунка кожи на пальце руки Клиента. Отпечаток пальца обеспечивает однозначную Верификацию Клиента.

Пароль - комбинация символов (цифр), служащая для Верификации Клиента в Мобильном устройстве Apple. Пароль обеспечивает однозначную Верификацию Клиента в Мобильном устройстве Apple. Пароль используется многократно, и может быть изменен Клиентом самостоятельно неограниченное количество раз.

Платежная система - совокупность организаций, взаимодействующих по правилам платежной системы в целях осуществления перевода денежных средств.

ПИН-код – персональный идентификационный номер, устанавливаемый / изменяемый Клиентом с использованием услуги по установке / смене ПИН-кода, для совершения операций/платежа с использованием Карты или ее реквизитов. ПИН-код подтверждает принадлежность Карты Клиенту и является аналогом собственноручной подписи (АСП) Клиента. Ввод ПИН-кода при совершении операции с использованием Карты является для Банка подтверждением факта совершения операции/платежа Клиентом. ПИН-код не используется при совершении операций в сети Интернет.

Правила по Карте - Условия дистанционного банковского обслуживания физических лиц в АКБ «ТЕНДЕР-БАНК» (АО) с использованием Системы ДБО «ТЕНДЕР-БАНК-Онлайн» (в действующей редакции);

Простая электронная подпись – электронная подпись, которая посредством использования Одноразового пароля / Пароля / Отпечатка пальца, подтверждает факт совершения определённого действия Клиентом в Системе Apple Pay (платеж в Системе Apple Pay, регистрация Карты в Apple Wallet).

Клиент признает, что электронный документ, сформированный для осуществления платежа посредством Системы Apple Pay и подписанный Простой электронной подписью, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью.

Система Apple Pay – система мобильных платежей от корпорации Apple Inc. Система Apple Pay совместима с существующими бесконтактными считывателями MasterCard PayPass. Она позволяет Клиенту оплачивать покупки при помощи беспроводной связи Мобильного устройства Apple без физического использования Карты. С помощью Системы Apple Pay владельцы Мобильных устройств Apple могут оплачивать покупки по технологии NFC («ближняя бесконтактная связь») в сочетании с программой/приложением Apple Wallet и Touch ID. Система Apple Pay позволяет Мобильным устройствам Apple осуществлять платежи в торгово-сервисных предприятиях и интернете. Клиент может выполнять платежи с СКС, используя беспроводную связь с Мобильного устройства Apple. Использование Системы Apple Pay осуществляется в соответствии с настоящими Условиями, Правилами по Карте и Тарифами.

СКС – специальный карточный счет, открытый Банком на имя Клиента, и предназначенный для проведения расчетов с использованием Карты или ее реквизитов. СКС для Клиента является текущим счетом и предназначен для проведения расчетов с использованием Карты или ее реквизитов, не связанных с осуществлением предпринимательской деятельности или частной практики.

Тарифы – Тарифы для физических лиц в АКБ «ТЕНДЕР-БАНК» (АО), являются неотъемлемой частью настоящих Условий.

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

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

Условия по Карте - Условия выпуска и обслуживания банковских карт Международной платежной системы MasterCard АКБ «ТЕНДЕР-БАНК» (АО) (в действующей редакции).

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)

Push-уведомления – краткие уведомления, всплывающие на экране Мобильного устройства Apple. Push-уведомления могут поступать от Банка, от Системы Apple Pay исключительно при наличии доступа к сети интернет.

Touch ID — дактилоскопический датчик/сканер Отпечатков пальцев, разработанный корпорацией Apple Inc., и предустановленный в Мобильных устройствах Apple. Touch ID позволяет Клиентам, в т.ч. использовать Отпечаток пальца в качестве подтверждения покупки в App Store, iTunes Store и iBooks Store.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Предметом договора, заключенного Клиентом путем присоединения к настоящим Условиям является оказание Банком Клиенту услуг по проведению расчетов по операциям, совершенным с использованием реквизитов Карты в Системе Apple Pay.

2.2. Заключение договора осуществляется путем присоединения к настоящим Условиям в момент регистрации Карты в Apple Wallet. При этом, фиксация присоединения Клиента к договору осуществляется

Банком в электронном виде в аппаратно-программном комплексе Банка в момент получения акцепта Клиента настоящих Условий. Присоединяясь к настоящим Условиям, Клиент подтверждает, что является непосредственным держателем Карты. Акцепт Клиента хранится в аппаратно-программном комплексе Банка.

Информация из аппаратно-программного комплекса Платежной системы, Банка и корпорации Apple Inc. может использоваться в качестве доказательств при рассмотрении споров, в том числе в судебном порядке.

2.3. Настоящие Условия определяют:

- процесс регистрации Карты в Apple Wallet, при котором Клиент принимает настоящие Условия полностью;
- порядок совершения и подтверждения операции, совершенной Клиентом в Системе Apple Pay;
- ответственность Клиента и Банка при осуществлении операций в Системе Apple Pay;
- требования к безопасности использования Мобильного устройства Apple при совершении платежей с использованием Карты в Системе Apple Pay.

2.4. Банк не является провайдером в Системе Apple Pay, и не предоставляет программное обеспечение (приложение Apple Wallet), установленное на Мобильном устройстве Клиента, в котором хранится Токен (DPAN).

2.5. Банк не взимает комиссию за использование Карт в Системе Apple Pay.

2.6. Настоящие Условия действуют до расторжения договора по Карте.

2.7. Прекращение действия настоящих Условий не влияет на юридическую силу и действительность распоряжений, направленных в Банк Клиентом до прекращения действия Условий.

2.8. Использование Системы Apple Pay в POS-терминалах возможно только в случае он-лайн Авторизации платежей.

2.9. Обслуживание Карты осуществляется в соответствии с Правилами по Карте / Условиями по Карте, а также в соответствии с законодательством Российской Федерации или правилами Платежной системы MasterCard WorldWide.

2.10. В случае несоответствия между любыми положениями настоящих Условий и законодательством Российской Федерации или правилами Платежной системы MasterCard WorldWide, Банк имеет право изменить Условия в одностороннем порядке, с целью приведения их в соответствие с законодательством РФ и/или правилами Платежной системы MasterCard WorldWide.

3. РЕГИСТРАЦИЯ КАРТ В APPLE WALLET

3.1. Для осуществления расчетов через Систему Apple Pay Клиенту необходимо зарегистрировать в Apple Wallet Карту одним из способов:

- используя iTunes с автоматическим заполнением Номера Карты;
- используя iSight (камера) с автоматическим заполнением Номера Карты;
- ввод Номера Карты вручную;
- иной способ при наличии технической возможности.

3.2. Для подтверждения действительности Карты осуществляется Верификации Карты с помощью CVC2. Карта должна быть активна, иметь не истекший срок действия.

3.3. После ввода Номера Карты одним из указанных в п.3.1. настоящих Условий способов, при необходимости дополнительной проверки Клиента Банком (по усмотрению Банка), осуществляется Верификация Клиента и активация Токена с использованием Простой электронной подписи одним из способов:

- путём ввода Клиентом Одноразового пароля, полученного в Push-уведомлении или СМС-сообщении на номер мобильного телефона Клиента, зафиксированный в информационных системах Банка.
- по факту успешной регистрации Карты в Apple Wallet, в защищенном хранилище Мобильного устройства Apple формируется и хранится Токен.

Токен позволяет однозначно идентифицировать Карту, используемую при совершении платежей в Системе Apple Pay.

По факту успешной регистрации Карты в Apple Wallet Система Apple Pay направляет Клиенту соответствующее Push-уведомление.

3.4. Одну Карту можно зарегистрировать в Apple Wallet не более чем на 20 (Двадцати) Мобильных устройствах Apple.

3.5. На одно Мобильное устройство Apple возможно зарегистрировать до 8 (восьми) Карт[1].

3.6. Клиент может самостоятельно удалить одну или несколько Карт из Apple Wallet, с помощью кнопки «удалить».

3.7. Изображение Карты в Apple Wallet может не соответствовать реальному дизайну Карты, и содержать маскированный Номер Карты (отображены 4 последние цифры Номера карты).

[1] Данный параметр может меняться по решению Apple Inc.

4. ПОДТВЕРЖДЕНИЕ ОПЕРАЦИИ КЛИЕНТА

4.1. Платежи в Системе Apple Pay могут осуществляться:

- через POS-терминал, оснащенный технологией NFC («ближняя бесконтактная связь»);
- в мобильных приложениях на Мобильном устройстве Apple, поддерживающих расчеты через Систему Apple Pay.

4.2. Если платеж совершен через POS-терминал, оснащенный технологией NFC, то подтверждение платежа осуществляется:

- до 1000 (Одной тысячи) рублей - с помощью Touch ID на Мобильном устройстве Apple, либо (в случае такой технической необходимости (невозможно отсканировать палец, искажен Отпечаток пальца и т.д.)) вводом пароля от Мобильного устройства Apple;
- свыше 1000 (Одной тысячи) рублей – дополнительно к вышеуказанным способам подтверждения платежа, Клиент должен в POS-терминале ввести ПИН-код Карты.

4.3. Если платеж совершен в мобильном приложении, поддерживающем Систему Apple Pay, то подтверждение платежа осуществляется с помощью Touch ID на Мобильном устройстве Apple, либо (в случае такой технической необходимости (невозможно отсканировать палец, искажен Отпечаток пальца и т.д.)) вводом пароля от Мобильного устройства Apple.

4.4. При наличии 2 (Двух) и более Карт в Apple Wallet, в том числе других банков-эмитентов, Клиент должен выбрать Карту, с использованием которой будут совершаться платежи в Системе Apple Pay.

4.5. В Apple Wallet фиксируются 10 (Десять)[2] последних операций по каждой Карте, содержащейся в Apple Wallet.

5. БЛОКИРОВКА ТОКЕНА / МОБИЛЬНОГО УСТРОЙСТВА APPLE

5.1. В случае утраты Карты Клиент обязан самостоятельно осуществить блокировку Карты в Мобильном Банке, в Банк-Клиент для частных лиц, либо заблокировать Карты по звонку в контакт-центр Банка.

По факту блокировки Карты, блокируются все Токены для данной Карты на всех Мобильных устройствах Apple с целью недопущения совершения расчетов в Системе Apple Pay.

5.2. В случае утраты Мобильного устройства Apple, Клиенту необходимо обратиться в Банк с целью блокировки Токена, содержащегося на данном Мобильном устройстве Apple.

В данном случае Банк блокирует только Токен, содержащийся на данном Мобильном устройстве Apple.

6. ТРЕБОВАНИЯ К БЕЗОПАСНОСТИ

6.1. Организационные меры по защите информации, реализуемые Клиентом:

- не оставлять Мобильное устройство Apple без присмотра;
- обеспечить соответствующий уровень безопасности на Мобильном устройстве Apple, используя Пароли, Touch ID и другие возможные методы блокировки/разблокировки Мобильного устройства Apple;
- убедиться, что на Мобильном устройстве Apple не зарегистрированы Отпечатки пальцев другого лица;
- не разглашать третьим лицам регистрационные данные от Мобильного устройства Apple, такие как Apple ID, Пароль. Это конфиденциальная информация;
- удалить все личные данные и финансовую информацию со старого Мобильного устройства Apple, если прекращено его использование;
- обратиться в Банк по номеру телефона, напечатанному на оборотной стороне Карты, либо по номеру телефона Банка, указанному на сайте Банка (http://www.tenderbank.ru), как можно скорее, в случае подозрений на любое несанкционированное использование Мобильного устройства Apple, а также, если Мобильное устройство Apple было взломано, потеряно или украдено.

Необходимо изменить учетные данные в Мобильном устройстве Apple, чтобы избежать несанкционированного использования Карт;

- не блокировать любые функции безопасности, предусмотренные приложениями Мобильных устройств Apple, для использования этих функций и процедур безопасности для защиты всех Карт, зарегистрированных в Apple Wallet;
- создать сложный Пароль;
- удалять информацию о Картах в Apple Wallet при передаче Мобильного устройства Apple третьим лицам.
- не подвергать Мобильное устройство Apple операциям повышения привилегий / взлома операционной системы устройства (jail-break).

[2] Данный параметр может меняться по решению Apple Inc.

7. ПРАВА И ОБЯЗАННОСТИ СТОРОН

7.1. Банк обязан:

7.1.1. Исполнять распоряжения Клиента по операциям, совершенным с использованием реквизитов Карты, в Системе Apple Pay;

7.1.2. принять все возможные меры к недопущению приема распоряжений с использованием реквизитов Карты в Системе Apple Pay без предварительной успешной Верификации Клиента (при необходимости ее проведения по решению Банка);

7.1.3. незамедлительно, но не позднее 30 (тридцати) минут с момента получения обращения Клиента об утрате Мобильного устройства Apple, компрометации Пароля и (или) утраты контроля над SIM-картой заблокировать Токены на данном Мобильном устройстве Apple. При обращении Клиента по телефону, установление личности Клиента осуществляется в соответствии с внутренними регламентными документами Банка;

7.1.4. в случае неисполнения Банком своевременно и должным образом обязанности, предусмотренной п.7.1.3. Условий, при поступлении от Клиента обращения об утрате Мобильного устройства Apple, Компрометации Пароля и (или) утраты контроля над SIM-картой, возместить Клиенту суммы операций, совершенных без согласия Клиента после получения от Клиента обращения;

7.1.5. возместить Клиенту суммы операций, которые были совершены при неуспешной Верификации Клиента (при необходимости ее проведения по решению Банка);

7.1.6. осуществлять консультирование Клиента по вопросам регистрации Карт в Apple Wallet;

7.1.7. в целях исполнения требований законодательства и обеспечения безопасности денежных средств Клиента, информировать Клиентов о совершении каждой операции, совершенной с использованием Карты в Системе Apple Pay путем предоставления выписки по СКС при обращении Клиента в офис Банка или при ее формировании Клиентом через Банк-Клиент для частных лиц АКБ «ТЕНДЕР-БАНК» (АО)/ Мобильный банк.

В случае если Клиент подключил услугу «SMS-инфо», Банк направляет уведомления о совершении каждой операции с использованием Карты в виде SMS-сообщения на номер мобильного телефона Клиента, указанный в информационных системах Банка. Также информация об операциях, совершенных с использованием Карты в Системе Apple Pay, предоставляется Клиентам при обращении в контакт-центр Банка по телефону. Обязанность по информированию считается исполненной при предоставлении Клиенту любым из вышеперечисленных способов информации о совершенных Операциях по СКС;

7.1.8. фиксировать и хранить, направленные Клиенту SMS-сообщения, содержащие информацию об операциях, совершенных с использованием реквизитов Карты в Системе Apple Pay, не менее 3 (Трех) лет;

7.1.9. фиксировать и хранить, полученные от Клиента обращения по телефонной связи по номеру телефона Банка, указанному на сайте Банка (http://www.tenderbank.ru), а также полученные путем подачи заявления в офис Банка, об утрате Мобильного устройства Apple, компрометации Пароля и (или) утраты контроля над SIM-картой не менее 3 (Трех) лет и 60 (Шестидесяти) дней соответственно;

7.1.10. обеспечить конфиденциальность информации об операциях, совершенных с использованием реквизитов Карты в Системе Apple Pay. При этом, Банк не отвечает за конфиденциальность информации, хранящейся на Мобильном устройстве Apple в соответствии с п. 4.5 настоящих Условий;

7.1.11. предоставлять по письменному требованию Клиенту документы, связанные с совершением Клиентом операций в Системе Apple Pay, с использованием Карты, в срок не позднее 30 дней со дня получения Банком соответствующего запроса.

7.2. Банк имеет право:

7.2.1. не исполнять распоряжения Клиента, совершенные с использованием Карты в Системе Apple Pay в случае:

- если Верификация Клиента / Верификация Карты произошла неуспешно;
- если Клиентом не соблюдены требования законодательства Российской Федерации, настоящих Условий.

7.2.2. если иное не предусмотрено законодательством Российской Федерации в одностороннем порядке изменять настоящие Условия, с уведомлением Клиента о таких изменениях не позднее, чем за 5 (Пять) календарных дней до вступления изменений в силу, путем размещения:

- информации на стендах в Офисах Банка;
- информации на официальном сайте Банка: http://www.tenderbank.ru;
- путем рассылки информационных сообщений Клиенту по электронной почте или по реквизитам Клиента, указанным в его Заявлении;
- информации в системе дистанционного банковского обслуживания «ТЕНДЕР-БАНК Онлайн»;

7.2.3. в целях обеспечения безопасности устанавливать ограничения по времени действия Одноразового пароля в пределах одного сеанса соединения (тайм-аут).

7.2.4. в установленных законодательством Российской Федерации случаях осуществлять в отношении Клиента контрольные и иные функции, возложенные на Банк законодательством Российской Федерации, в связи с чем запрашивать у Клиента любые необходимые документы и (или) письменные пояснения относительно характера и экономического смысла предполагаемых или совершенных операций с использованием реквизитов Карты в Системе Apple Pay;

7.2.5. в любой момент потребовать от Клиента подписания документов на бумажном носителе, эквивалентных по смыслу и содержанию переданным Клиентом и исполненным Банком распоряжений Клиента.

7.2.6. заблокировать, ограничить, приостановить или прекратить использование реквизитов Карты в Apple Wallet и платежей, совершенных с использованием реквизитов Карты в Системе Apple Pay в любое время без уведомления и по любой причине, в том числе, если Клиент нарушает настоящие Условия.

7.2.7. отказать Клиенту в регистрации Карты в Apple Wallet для совершения платежей в Системе Apple Pay при неуспешной Верификации Клиента / Карты;

7.2.8. по своему усмотрению удалить Токен, а также удалить Карту из Системы Apple Pay, в том числе в случае неисполнения Клиентом п.7.3.6. настоящих Условий.

7.3. Клиент обязан:

7.3.1. соблюдать положения настоящих Условий;

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

В случае утраты Клиентом Мобильного устройства Apple, Пароля, SIM-карты или наличия подозрений, что они используются третьими лицами, Клиент должен незамедлительно, после обнаружения указанных фактов, но не позднее дня, следующего за днем получения от Банка уведомления о совершенной операции, сообщить об этом Банку по телефонной связи по номеру телефона, указанному на сайте Банка (http://www.tenderbank.ru), путем подачи заявления во внутреннее структурное/обособленное подразделение Банка.

На основании сообщения, Банк в срок, указанный в п. 7.1.3. Условий, блокирует Токен.

Отсутствие предусмотренного настоящим пунктом сообщения со стороны Клиента лишает Клиента права на получение возмещения от Банка по операциям, совершенным без согласия Клиента.

7.3.3. в случае несанкционированного списания денежных средств с использованием реквизитов Карты в Системе Apple Pay, Клиент должен сотрудничать с Банком в данном расследовании и предоставить в Банк следующие документы:

- заявление по установленной в Банке форме либо, по усмотрению Банка, в свободной форме с указанием даты и времени поступления SMS-сообщения / Push-уведомления о несанкционированной операции и с подробным описанием данной операции;
- подтверждение непричастности Клиента к совершению операции, например: материалы расследований правоохранительных органов, если по факту совершения несанкционированной операции имело место возбуждения уголовного дела компетентными органами и др.;
- документы из торговой организации;
- иные документы и информацию, которые имеют отношение к спорной ситуации или которые могут быть разумно затребованы Банком в рамках рассмотрения заявлений о несанкционированных списаниях.

7.3.4. регулярно обращаться в Банк за получением информации об имевших место изменениях и дополнениях в настоящие Условия.

7.3.5. контролировать соответствие суммы операции и текущего остатка на СКС и осуществлять операции в Системе Apple Pay только в пределах этого остатка, за исключением случаев предоставления Банком кредитного лимита, что регулируется отдельным договором. При отправке поручений контролировать достаточность средств на СКС для одновременного списания комиссии за данную операцию в соответствии с Тарифами (при наличии).

7.3.6. в течение 3 (трех) рабочих дней сообщать Банку об изменении номера мобильного телефона Клиента, прекращении обслуживания номера мобильного телефона Клиента оператором сотовой связи или замены SIM-карты. Банк, получив указанную информацию, имеет право приостановить предоставление Услуги до момента подтверждения принадлежности номера мобильного телефона Клиенту, путем обращения Клиента в офис Банка.

7.3.7. предоставлять запрашиваемые Банком на основании п.7.2.4. Условий документы и (или) письменные пояснения относительно характера и экономического смысла совершенных операций в Системе Apple Pay.

7.3.8. исполнять требования, изложенные в разделе 6 Условий.

7.4. Клиент имеет право:

7.4.1. обращаться в Банк для получения консультаций по работе в Системе Apple Pay.

7.4.2. приостановить действие Карты / Токена, обратившись в Банк лично или по телефону. При обращении по телефону, идентификация Клиента осуществляется в соответствии с внутренними регламентными документами Банка.

7.4.3. обращаться в Банк с заявлениями, в том числе при возникновении споров, связанных с операциями, совершенными с использованием реквизитов Карты в Системе Apple Pay, а также получать информацию о результатах рассмотрения заявлений, в том числе в письменной форме, в срок не более 30 дней со дня получения Банком таких заявлений.

8. ОТВЕТСТВЕННОСТЬ СТОРОН

8.1. Ответственность Клиента.

Клиент несет ответственность за:

- сохранение конфиденциальности Apple ID, Пароля и других средств Верификации Клиента.
- использование Мобильного устройства Apple третьими лицами;
- за операции, совершенные Клиентом в Системе Apple Pay с использованием реквизитов Карты, зарегистрированной в Apple Wallet на Мобильном устройстве Apple Клиента.
- нарушение требований к технической защите Мобильного устройства Apple, указанных в разделе 6 настоящих Условий, в том числе в случаях, когда Клиент использует Мобильное устройство Apple, которое было подвергнуто операциям повышения привилегий / взлома операционной системы устройства (jail-break, rooting).

8.2. Ответственность Банка.

8.2.1. Банк не несет ответственности:

- за работу Системы Apple Pay,
- за отсутствие возможности совершения в Системе Apple Pay операций,
- за любой блок, приостановление, аннулирование или прекращение использования Карты в Системе Apple Pay,
- за конфиденциальность информации, хранящейся на Мобильном устройстве Apple, в том числе в Apple Wallet.

9. ПРОЧИЕ УСЛОВИЯ

9.1. Принимая настоящие Условия, Клиент дает согласие на получение от Банка SMS-сообщений / Push-уведомлений, необходимых для совершения платежей в Системе Apple Pay, на Мобильное устройство Apple;

9.2. Принимая настоящие Условия, Клиент понимает и согласен с тем, что:

- доступ, использование и возможность совершения платежей посредством реквизитов Карты в Системе Apple Pay зависит исключительно от Системы Apple Pay, от состояния сетей беспроводной связи, используемой Системой Apple Pay.
- 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 компании Apple Inc.
- Банк не несет ответственности за поддержку операционной системы (iOS) Мобильного устройства Apple.

9.3. Товарные знаки Apple, Apple Pay, Apple Wallet, Touch ID, App Store, iTunes Store, iBooks Store, iOS, iPhone, iPad являются товарными знаками компании Apple Inc., зарегистрированными в США и других странах и регионах.

Условия
использования расчетных карт АКБ «ТЕНДЕР-БАНК» (АО)
в Системе Google Pay

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

ID – уникальный идентификатор Клиента как пользователя Мобильного устройства.

Авторизация платежа - процедура получения подтверждения Банком на проведение операции с использованием Карты посредством информационного обмена между участниками расчетов.

Банк – АКБ «ТЕНДЕР-БАНК» (АО). Банк осуществляет выпуск Карт, и обязуется обеспечивать расчеты по операциям, совершенным Клиентами с использованием Карт в Системе Google Pay.

Верификация Карты - процедура дополнительной проверки Банком Карты Клиента, осуществляемая с целью снижения рисков проведения мошеннической операции по Карте Клиента. Верификация Карты осуществляется по Технологии CVC2/CVV2 кода.

Верификация Клиента - процедура подтверждения полномочий (предоставление прав доступа) Клиента.

При регистрации Карты в Google Pay, Верификация Клиента может осуществляться путем ввода Клиентом 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 Клиента осуществляется путем ввода Клиентом Пароля или Отпечатка пальца и/или дополнительным вводом ПИН-кода Карты (при платежах через POS-терминал).

Банк-Клиент для частных лиц – используемые Банком организационно-технические системы дистанционного банковского обслуживания физических лиц, при котором доступ к счетам Клиентов Банка, в том числе для совершения операций по ним, предоставляется в любое время и с любого компьютера (иного устройства), имеющего доступ в интернет. Обслуживание Клиента Банка посредством Банк-Клиента для частных лиц осуществляется в соответствии с Условиями дистанционного банковского обслуживания физических лиц в АКБ «ТЕНДЕР-БАНК» (АО) с использованием Системы ДБО «ТЕНДЕР-БАНК-Онлайн» (в действующей редакции).

Карта – международная банковская карта Платежной системы MasterCard WorldWide, выпускаемая Банком в качестве средства для составления расчетных и иных документов, подлежащих оплате, осуществления операций по СКС и получения информации о СКС.

Клиент – физическое лицо, являющееся держателем Карты, и имеющее Мобильное устройство.

Мобильное устройство – устройство (смартфон, планшет, часы) с поддержкой Системы Google Pay.

Мобильный Банк – используемая Банком организационно-техническая система дистанционного банковского обслуживания физических лиц, при котором доступ к счетам Клиентов, в том числе для совершения операций по ним, предоставляется в любое время с мобильного устройства, имеющего доступ в интернет. Обслуживание Клиента Банка посредством Мобильного Банка осуществляется в соответствии с Условиями дистанционного банковского обслуживания физических лиц в АКБ «ТЕНДЕР-БАНК» (АО) с использованием Системы ДБО «ТЕНДЕР-БАНК-Онлайн» (в действующей редакции).

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

Одноразовый пароль – комбинация символов в виде 6-ти цифр, генерируемая Банком при попытке зарегистрировать Карту в Google Pay, и направляемая Клиенту в виде Push-уведомления или СМС-сообщения на номер мобильного телефона Клиента, зафиксированный в информационных системах Банка.

Отпечаток пальца – однозначное цифровое представление рисунка кожи на пальце руки Клиента. Отпечаток пальца обеспечивает однозначную Верификацию Клиента.

Пароль - комбинация символов (цифр), служащая для Верификации Клиента в Мобильном устройстве. Пароль обеспечивает однозначную Верификацию Клиента в Мобильном устройстве. Пароль используется многократно, и может быть изменен Клиентом самостоятельно неограниченное количество раз.

Платежная система - совокупность организаций, взаимодействующих по правилам платежной системы в целях осуществления перевода денежных средств.

ПИН-код – персональный идентификационный номер, устанавливаемый / изменяемый Клиентом с использованием услуги по установке / смене ПИН-кода, для совершения операций/платежа с использованием Карты или ее реквизитов. ПИН-код подтверждает принадлежность Карты Клиенту и является аналогом собственноручной подписи (АСП) Клиента. Ввод ПИН-кода при совершении операции с использованием Карты

является для Банка подтверждением факта совершения операции/платежа Клиентом. ПИН-код не используется при совершении операций в сети Интернет.

Правила по Карте - Условия дистанционного банковского обслуживания физических лиц в АКБ «ТЕНДЕР-БАНК» (АО) с использованием Системы ДБО «ТЕНДЕР-БАНК-Онлайн» (в действующей редакции);

Простая электронная подпись – электронная подпись, которая посредством использования Одноразового пароля / Пароля / Отпечатка пальца, подтверждает факт совершения определённого действия Клиентом в Системе Google Pay (платеж в Системе Google Pay, регистрация Карты в Google Pay).

Клиент признает, что электронный документ, сформированный для осуществления платежа посредством Системы Google Pay и подписанный Простой электронной подписью, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью.

Система Google Pay – система мобильных платежей. Система Google Pay совместима с существующими бесконтактными считывателями MasterCard PayPass. Она позволяет Клиенту оплачивать покупки при помощи беспроводной связи Мобильного устройства без физического использования Карты. С помощью Системы Google Pay владельцы Мобильных устройств могут оплачивать покупки по технологии NFC («ближняя бесконтактная связь») в сочетании с программой/приложением Google Pay и Touch ID. Система Google Pay позволяет Мобильным устройствам осуществлять платежи в торгово-сервисных предприятиях и интернете. Клиент может выполнять платежи с СКС, используя беспроводную связь с Мобильного устройства. Использование Системы Google Pay осуществляется в соответствии с настоящими Условиями, Правилами по Карте и Тарифами.

СКС – специальный карточный счет, открытый Банком на имя Клиента, и предназначенный для проведения расчетов с использованием Карты или ее реквизитов. СКС для Клиента является текущим счетом и предназначен для проведения расчетов с использованием Карты или ее реквизитов, не связанных с осуществлением предпринимательской деятельности или частной практики.

Тарифы – Тарифы для физических лиц в АКБ «ТЕНДЕР-БАНК» (АО), являются неотъемлемой частью настоящих Условий.

Токен (DPAN) – цифровое представление Карты, которое формируется по факту регистрации Карты в Google Pay, и которое хранится в зашифрованном виде в защищенном хранилище Мобильного устройства.

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

Условия по Карте - Условия выпуска и обслуживания банковских карт Международной платежной системы MasterCard АКБ «ТЕНДЕР-БАНК» (АО) (в действующей редакции).

Google Pay — предустановленная на Мобильном устройстве 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)

Push-уведомления – краткие уведомления, всплывающие на экране Мобильного устройства. Push-уведомления могут поступать от Банка, от Системы Google Pay исключительно при наличии доступа к сети интернет.

Touch ID — дактилоскопический датчик/сканер Отпечатков пальцев, разработанный корпорацией Google, и предустановленный в Мобильных устройствах. Touch ID позволяет Клиентам, в т.ч. использовать отпечаток пальца в качестве подтверждения покупки.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Предметом договора, заключенного Клиентом путем присоединения к настоящим Условиям является оказание Банком Клиенту услуг по проведению расчетов по операциям, совершенным с использованием реквизитов Карты в Системе Google Pay.

2.2. Заключение договора осуществляется путем присоединения к настоящим Условиям в момент регистрации Карты в Google Pay. При этом фиксация присоединения Клиента к договору осуществляется Банком в электронном виде в аппаратно-программном комплексе Банка в момент получения акцепта Клиента настоящих Условий. Присоединяясь к настоящим Условиям, Клиент подтверждает, что является непосредственным держателем Карты. Акцепт Клиента хранится в аппаратно-программном комплексе Банка.

Информация из аппаратно-программного комплекса Платежной системы, Банка и корпорации Google может использоваться в качестве доказательств при рассмотрении споров, в том числе в судебном порядке.

2.3. Настоящие Условия определяют:

- процесс регистрации Карты в Google Pay, при котором Клиент принимает настоящие Условия полностью;
- порядок совершения и подтверждения операции, совершенной Клиентом в Системе Google Pay;
- ответственность Клиента и Банка при осуществлении операций в Системе Google Pay;

- требования к безопасности использования Мобильного устройства при совершении платежей с использованием Карты в Системе Google Pay.

2.4. Банк не является провайдером в Системе Google Pay, и не предоставляет программное обеспечение (приложение Google Pay), установленное на Мобильном устройстве Клиента, в котором хранится Токен (DPAN).

2.5. Банк не взимает комиссию за использование Карт в Системе Google Pay.

2.6. Настоящие Условия действуют до расторжения договора по Карте.

2.7. Прекращение действия настоящих Условий не влияет на юридическую силу и действительность распоряжений, направленных в Банк Клиентом до прекращения действия Условий.

2.8. Использование Системы Google Pay в POS-терминалах возможно только в случае он-лайн Авторизации платежей.

2.9. Обслуживание Карты осуществляется в соответствии с Правилами по Карте / Условиями по Карте, а также в соответствии с законодательством Российской Федерации или правилами Платежной системы MasterCard WorldWide.

2.10. В случае несоответствия между любыми положениями настоящих Условий и законодательством Российской Федерации или правилами Платежной системы MasterCard WorldWide, Банк имеет право изменить Условия в одностороннем порядке, с целью приведения их в соответствие с законодательством Российской Федерации и/или правилами Платежной системы MasterCard WorldWide.

3. РЕГИСТРАЦИЯ КАРТ В GOOGLE PAY

3.1. Для осуществления расчетов через Систему Google Pay Клиенту необходимо зарегистрировать в Google Pay Карту одним из способов:

- ввод Номера Карты вручную;
- иной способ при наличии технической возможности.

3.1. Для подтверждения действительности Карты осуществляется Верификации Карты с помощью CVC2. Карта должна быть активна, иметь не истекший срок действия.

3.2. После ввода Номера Карты одним из указанных в п.3.1. настоящих Условий способов, при необходимости дополнительной проверки Клиента Банком (по усмотрению Банка), осуществляется Верификация Клиента и активация Токена с использованием Простой электронной подписи одним из способов:

- путём ввода Клиентом Одноразового пароля, полученного в Push-уведомлении или СМС-сообщении на номер мобильного телефона Клиента, зафиксированный в информационных системах Банка.
- По факту успешной регистрации Карты в Google Pay, в защищенном хранилище Мобильного устройства формируется и хранится Токен.

Токен позволяет однозначно идентифицировать Карту, используемую при совершении платежей в Системе Google Pay.

По факту успешной регистрации Карты в Google Pay, Система Google Pay направляет Клиенту соответствующее Push-уведомление.

3.3. Одну Карту можно зарегистрировать в Google Pay не более чем на 20 (Двадцати) Мобильных устройствах.

3.4. На одно Мобильное устройство возможно зарегистрировать до 8 (восьми) Карт[3].

3.5. Клиент может самостоятельно удалить одну или несколько Карт из Google Pay, с помощью кнопки «удалить».

3.6. Изображение Карты в Google Pay может не соответствовать реальному дизайну Карты, и содержать маскированный Номер Карты (отображены 4 последние цифры Номера карты).

4. ПОДТВЕРЖДЕНИЕ ОПЕРАЦИИ КЛИЕНТА

4.1. Платежи в Системе Google Pay могут осуществляться:

- Через POS-терминал, оснащенный технологией NFC («ближняя бесконтактная связь»);
- В мобильных приложениях на Мобильном устройстве, поддерживающих расчеты через Систему Google Pay.

4.2. Если платеж совершен через POS-терминал, оснащенный технологией NFC, то подтверждение платежа осуществляется:

- До 1000 (Одной тысячи) рублей - с помощью Touch ID на Мобильном устройстве, либо (в случае такой технической необходимости (невозможно отсканировать палец, искажен Отпечаток пальца и т.д.)) вводом пароля от Мобильного устройства;
- Свыше 1000 (Одной тысячи) рублей – дополнительно к вышеуказанным способам подтверждения платежа, Клиент должен в POS-терминале ввести ПИН-код Карты.

---

[3] Данный параметр может меняться по решению Google.

4.3. Если платеж совершен в мобильном приложении, поддерживающем Систему Google Pay, то подтверждение платежа осуществляется с помощью Touch ID на Мобильном устройстве, либо (в случае такой технической необходимости (невозможно отсканировать палец, искажен Отпечаток пальца и т.д.)) вводом пароля от Мобильного устройства.

4.4. При наличии 2 (Двух) и более Карт в Google Pay, в том числе других банков-эмитентов, Клиент должен выбрать Карту, с использованием которой будут совершаться платежи в Системе Google Pay.

4.5. В Google Pay фиксируются 10 (Десять)[4] последних операций по каждой Карте, содержащейся в Google Pay.

5. БЛОКИРОВКА ТОКЕНА / МОБИЛЬНОГО УСТРОЙСТВА

5.1. В случае утраты Карты Клиент обязан самостоятельно осуществить блокировку Карты в Мобильном Банке, в Банк-Клиент для частных лиц, либо заблокировать Карты по звонку в контакт-центр Банка.

По факту блокировки Карты, блокируются все Токены для данной Карты на всех Мобильных устройствах с целью недопущения совершения расчетов в Системе Google Pay.

5.2. В случае утраты Мобильного устройства, Клиенту необходимо обратиться в Банк с целью блокировки Токена, содержащегося на данном Мобильном устройстве.

В данном случае Банк блокирует только Токен, содержащийся на данном Мобильном устройстве.

6. ТРЕБОВАНИЯ К БЕЗОПАСНОСТИ

6.1. Организационные меры по защите информации, реализуемые Клиентом:

- не оставлять Мобильное устройство без присмотра;
- обеспечить соответствующий уровень безопасности на Мобильном устройстве, используя Пароли, Touch ID и другие возможные методы блокировки/разблокировки Мобильного устройства;
- убедиться, что на Мобильном устройстве не зарегистрированы Отпечатки пальцев другого лица;
- не разглашать третьим лицам регистрационные данные от Мобильного устройства, такие как ID, Пароль. Это конфиденциальная информация;
- удалить все личные данные и финансовую информацию со старого Мобильного устройства, если прекращено его использование;
- обратиться в Банк по номеру телефона, напечатанному на оборотной стороне Карты, либо по номеру телефона Банка, указанному на сайте Банка (http://www.tenderbank.ru), как можно скорее, в случае подозрений на любое несанкционированное использование Мобильного устройства, а также, если Мобильное устройство было 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, зарегистрированных в Google Pay;
- создать сложный Пароль;
- удалять информацию о Картах в Google Pay при передаче Мобильного устройства третьим лицам.
- не подвергать Мобильное устройство операциям повышения привилегий (в том числе путем получения ROOT-прав) / взлома операционной системы устройства.
- Приложение Google Pay устанавливать с официального магазина приложений Play Маркет.

7. ПРАВА И ОБЯЗАННОСТИ СТОРОН

7.1. Банк обязан:

7.1.1. Исполнять распоряжения Клиента по операциям, совершенным с использованием реквизитов Карты, в Системе Google Pay;

7.1.2. принять все возможные меры к недопущению приема распоряжений с использованием реквизитов Карты в Системе Google Pay без предварительной успешной Верификации Клиента (при необходимости ее проведения по решению Банка);

7.1.3. незамедлительно, но не позднее 30 (Тридцати) минут с момента получения обращения Клиента об утрате Мобильного устройства, компрометации Пароля и (или) утраты контроля над SIM-картой заблокировать Токены на данном Мобильном устройстве. При обращении Клиента по телефону, установление личности Клиента осуществляется в соответствии с внутренними регламентными документами Банка;

---

[4] Данный параметр может меняться по решению Google.

7.1.4. в случае неисполнения Банком своевременно и должным образом обязанности, предусмотренной п.7.1.3. Условий, при поступлении от Клиента обращения об утрате Мобильного устройства, Компрометации Пароля и (или) утраты контроля над SIM-картой, возместить Клиенту суммы операций, совершенных без согласия Клиента после получения от Клиента обращения;

7.1.5. возместить Клиенту суммы операций, которые были совершены при неуспешной Верификации Клиента (при необходимости ее проведения по решению Банка);

7.1.6. осуществлять консультирование Клиента по вопросам регистрации Карт в Google Pay;

7.1.7. в целях исполнения требований законодательства и обеспечения безопасности денежных средств Клиента, информировать Клиентов о совершении каждой операции, совершенной с использованием Карты в Системе Google Pay путем предоставления выписки по СКС при обращении Клиента в офис Банка или при ее формировании Клиентом через Банк-Клиент для частных лиц АКБ «ТЕНДЕР-БАНК» (АО)/ Мобильный банк.

В случае если Клиент подключил услугу «SMS-инфо», Банк направляет уведомления о совершении каждой операции с использованием Карты в виде SMS-сообщения на номер мобильного телефона Клиента, указанный в информационных системах Банка. Также информация об операциях, совершенных с использованием Карты в Системе Google Pay, предоставляется Клиентам при обращении в контакт-центр Банка по телефону. Обязанность по информированию считается исполненной при предоставлении Клиенту любым из вышеперечисленных способов информации о совершенных Операциях по СКС;

7.1.8. фиксировать и хранить, направленные Клиенту SMS-сообщения, содержащие информацию об операциях, совершенных с использованием реквизитов Карты в Системе Google Pay, не менее 3 (Трех) лет;

7.1.9. фиксировать и хранить, полученные от Клиента обращения по телефонной связи по номеру телефона Банка, указанному на сайте Банка (http://www.tenderbank.ru), а также полученные путем подачи заявления в офис Банка, об утрате Мобильного устройства, компрометации Пароля и (или) утраты контроля над SIM-картой не менее 3 (трех) лет и 60 (шестидесяти) дней соответственно;

7.1.10. обеспечить конфиденциальность информации об операциях, совершенных с использованием реквизитов Карты в Системе Google Pay. При этом Банк не отвечает за конфиденциальность информации, хранящейся на Мобильном устройстве в соответствии с п. 4.5 настоящих Условий;

7.1.11. предоставлять по письменному требованию Клиенту документы, связанные с совершением Клиентом операций в Системе Google Pay, с использованием Карты, в срок не позднее 30 дней со дня получения Банком соответствующего запроса.

7.2. Банк имеет право:

7.2.1. не исполнять распоряжения Клиента, совершенные с использованием Карты в Системе Google Pay в случае:

- если Верификация Клиента / Верификация Карты произошла неуспешно;
- если Клиентом не соблюдены требования законодательства Российской Федерации, настоящих Условий.

7.2.2. если иное не предусмотрено законодательством Российской Федерации в одностороннем порядке изменять настоящие Условия, с уведомлением Клиента о таких изменениях не позднее, чем за 5 (Пять) календарных дней до вступления изменений в силу, путем размещения:

- информации на стендах в Офисах Банка;
- информации на официальном сайте Банка: http://www.tenderbank.ru;
- путем рассылки информационных сообщений Клиенту по электронной почте или по реквизитам Клиента, указанным в его Заявлении;
- информации в системе дистанционного банковского обслуживания «ТЕНДЕР-БАНК Онлайн»;

7.2.3. в целях обеспечения безопасности устанавливать ограничения по времени действия Одноразового пароля в пределах одного сеанса соединения (тайм-аут);

7.2.4. в установленных законодательством Российской Федерации случаях осуществлять в отношении Клиента контрольные и иные функции, возложенные на Банк законодательством Российской Федерации, в связи с чем запрашивать у Клиента любые необходимые документы и (или) письменные пояснения относительно характера и экономического смысла предполагаемых или совершенных операций с использованием реквизитов Карты в Системе Google Pay;

7.2.5. в любой момент потребовать от Клиента подписания документов на бумажном носителе, эквивалентных по смыслу и содержанию переданным Клиентом и исполненным Банком распоряжений Клиента.

7.2.6. заблокировать, ограничить, приостановить или прекратить использование реквизитов Карты в Google Pay и платежей, совершенных с использованием реквизитов Карты в Системе Google Pay в любое время без уведомления и по любой причине, в том числе, если Клиент нарушает настоящие Условия.

7.2.7. отказать Клиенту в регистрации Карты в Google Pay для совершения платежей в Системе Google Pay при неуспешной Верификации Клиента / Карты;

7.2.8. по своему усмотрению удалить Токен, а также удалить Карту из Системы Google Pay, в том числе в случае неисполнения Клиентом п.7.3.6. настоящих Условий.

7.3. Клиент обязан:

7.3.1. соблюдать положения настоящих Условий;

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

В случае утраты Клиентом Мобильного устройства, Пароля, SIM-карты или наличия подозрений, что они используются третьими лицами, Клиент должен незамедлительно, после обнаружения указанных фактов, но не позднее дня, следующего за днем получения от Банка уведомления о совершенной операции, сообщить об этом Банку по телефонной связи по номеру телефона, указанному на сайте Банка (http://www.tenderbank.ru), путем подачи заявления во внутреннее структурное/обособленное подразделение Банка.

На основании сообщения, Банк в срок, указанный в п. 7.1.3. Условий, блокирует Токен.

Отсутствие предусмотренного настоящим пунктом сообщения со стороны Клиента лишает Клиента права на получение возмещения от Банка по операциям, совершенным без согласия Клиента.

7.3.3. в случае несанкционированного списания денежных средств с использованием реквизитов Карты в Системе Google Pay, Клиент должен сотрудничать с Банком в данном расследовании и предоставить в Банк следующие документы:

- заявление по установленной в Банке форме либо, по усмотрению Банка, в свободной форме с указанием даты и времени поступления SMS-сообщения / Push-уведомления о несанкционированной операции и с подробным описанием данной операции;
- подтверждение непричастности Клиента к совершению операции, например: материалы расследований правоохранительных органов, если по факту совершения несанкционированной операции имело место возбуждения уголовного дела компетентными органами и др.;
- документы из торговой организации;
- иные документы и информацию, которые имеют отношение к спорной ситуации или которые могут быть разумно затребованы Банком в рамках рассмотрения заявлений о несанкционированных списаниях.

7.3.4. регулярно обращаться в Банк за получением информации об имевших место изменениях и дополнениях в настоящие Условия.

7.3.5. контролировать соответствие суммы операции и текущего остатка на СКС и осуществлять операции в Системе Google Pay только в пределах этого остатка, за исключением случаев предоставления Банком кредитного лимита, что регулируется отдельным договором. При отправке поручений контролировать достаточность средств на СКС для одновременного списания комиссии за данную операцию в соответствии с Тарифами (при наличии).

7.3.6. в течение 3 (Трех) рабочих дней сообщать Банку об изменении номера мобильного телефона Клиента, прекращении обслуживания номера мобильного телефона Клиента оператором сотовой связи или замены SIM-карты. Банк, получив указанную информацию, имеет право приостановить предоставление Услуги до момента подтверждения принадлежности номера мобильного телефона Клиенту, путем обращения Клиента в офис Банка.

7.3.7. предоставлять запрашиваемые Банком на основании п.7.2.4. Условий документы и (или) письменные пояснения относительно характера и экономического смысла совершенных операций в Системе Google Pay.

7.3.8. исполнять требования, изложенные в разделе 6 Условий.

7.4. Клиент имеет право:

7.4.1. обращаться в Банк для получения консультаций по работе в Системе Google Pay.

7.4.2. приостановить действие Карты / Токена, обратившись в Банк лично или по телефону. При обращении по телефону, идентификация Клиента осуществляется в соответствии с внутренними регламентными документами Банка.

7.4.3. обращаться в Банк с заявлениями, в том числе при возникновении споров, связанных с операциями, совершенными с использованием реквизитов Карты в Системе Google Pay, а также получать информацию о результатах рассмотрения заявлений, в том числе в письменной форме, в срок не более 30 дней со дня получения Банком таких заявлений.

8. ОТВЕТСТВЕННОСТЬ СТОРОН

8.1. Ответственность Клиента.

Клиент несет ответственность за:

- сохранение конфиденциальности ID, Пароля и других средств Верификации Клиента.
- использование Мобильного устройства третьими лицами;

- за операции, совершенные Клиентом в Системе Google Pay с использованием реквизитов Карты, зарегистрированной в Google Pay на Мобильном устройстве Клиента.
- нарушение требований к технической защите Мобильного устройства, указанных в разделе 6 настоящих Условий, в том числе в случаях, когда Клиент использует Мобильное устройство, которое было подвергнуто операциям повышения привилегий (в том числе путем получения ROOT-прав) / взлома операционной системы устройства (rooting).

8.2. Ответственность Банка.

8.2.1. Банк не несет ответственности:

- за работу Системы Google Pay,
- за отсутствие возможности совершения в Системе Google Pay операций,
- за любой блок, приостановление, аннулирование или прекращение использования Карты в Системе Google Pay,
- за конфиденциальность информации, хранящейся на Мобильном устройстве, в том числе в Google Pay.

9. ПРОЧИЕ УСЛОВИЯ

9.1. Принимая настоящие Условия, Клиент дает согласие на получение от Банка SMS-сообщений / Push-уведомлений, необходимых для совершения платежей в Системе Google Pay, на Мобильное устройство;

9.2. Принимая настоящие Условия, Клиент понимает и согласен с тем, что:

- доступ, использование и возможность совершения платежей посредством реквизитов Карты в Системе Google Pay зависит исключительно от Системы Google Pay, от состояния сетей беспроводной связи, используемой Системой Google Pay.
- 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 компании Google.
- Банк не несет ответственности за поддержку операционной системы Мобильного устройства