БАНК ДОЛИНСК

Условия

Использования банковских карт КБ «Долинск» (АО) в системах мобильных платежей

(Версия 1.0)

г. Южно-Сахалинск

2018 год

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

Банк – КБ «Долинск» (АО).

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 Клиента в Google Pay верификация осуществляется путем ввода Клиентом Одноразового пароля, направленного на номер мобильного телефона Клиента. 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/ПИН-кодом приложения (при платежах через POS- терминал).

Интернет-банк – система Дистанционного Банковского Обслуживания Клиента через сеть Интернет (https://elf.faktura.ru/elf/app/?site=bankdolinsk). Обслуживание Клиента Банка посредством Интернет-Банка осуществляется в соответствии с Условиями предоставления услуги Интернет – Банк КБ «Долинск».

Карта – вид электронного средства платежа, предназначена для проведения операций по погашению кредитов, выданных Банком, а также иных операций с денежными средствами. В рамках настоящих Условий под понятие «Карта» попадают только карты Платежной системы MasterCard WorldWide.

Карточный счет - лицевой счет, открываемый в Банке Держателю карты, для отражения операций с использованием банковской карты или ее реквизитов, не связанных с осуществлением предпринимательской деятельности или частной практики.

Клиент – физическое лицо, являющееся держателем Карты, и имеющее Мобильное устройство, работающее на платформе Android.

Мобильное устройство – смартфоны с операционной системой Android версии 4.4 и выше и модулем бесконтактных платежей NFC. Google Pay поддерживается также на смарт-часах, оснащенных бесконтактным NFC-чипом и работающих на Android Wear 2.0. (список указан на сайте https://googleandroidpay.ru/).

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, к которому подключена услуга «СМС-информирование».

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

Пароль - комбинация символов (цифр и/или букв), 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.

ПИН-код – персональный идентификационный номер, устанавливаемый 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.

Условия по Карте – условия использования банковских карт Банка, определенные в публичном Договоре о выпуске и обслуживании кредитных банковских карт и (или) в публичном Договоре об открытии и ведении счета с использованием банковских карт.

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, подписанному собственноручной подписью.

Система Google Pay - система мобильных платежей от корпорации Google. Сервис основан на бесконтактной передаче данных, которая действует напрямую от устройства к терминалу.

Система мобильных платежей (далее СМП). (В зависимости от контекста термин может употребляться как в единственном, так и во множественном числе**) –** системы, разработанные и предоставленные сторонними организациями/провайдерами, для осуществления платежей с помощью банковских карт на мобильном устройстве с соответствующими техническими характеристиками.

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 СМП.

Google Pay – официальное приложение из PlayМаркет, установленное на устройство, работающее на платформе Android, обеспечивающее Токенизацию и хранение информации о Токенах.

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

Touch ID — дактилоскопический датчик/сканер Отпечатков пальцев, предустановленный в Мобильных устройствах. Touch ID позволяет Клиентам использовать Отпечаток пальца в качестве подтверждения покупки

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.2. Настоящие Условия определяют порядок оказания Банком Клиенту услуг по проведению расчетов по операциям, совершенным с использованием реквизитов Карты в Системах мобильных платежей.

2.3. Настоящие Условия являются соглашением между держателем Карты и Банком. В момент регистрации Карты в СМП Клиент присоединяется к настоящим Условиям.

Присоединяясь к настоящим Условиям, Клиент подтверждает, что является непосредственным держателем Карты. Акцепт Клиента хранится в банковском информационном комплексе.

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

2.4. Настоящие Условия определяют:

2.4.1. процесс регистрации Карты в СМП, при котором Клиент принимает настоящие Условия полностью;

2.4.2. порядок совершения и подтверждения операции, совершенной Клиентом в СМП;

2.4.3. ответственность Клиента и Банка при осуществлении операций в СМП;

2.4.4. требования к безопасности использования Мобильного устройства при совершении платежей с использованием Карты в СМП.

2.5. Банк не является провайдером в СМП и не предоставляет программное обеспечение, установленное на Мобильном устройстве Клиента, в котором хранится Токен (DPAN).

2.6. Настоящие Условия устанавливают правила использования Карт в СМП только в отношениях между Банком и Клиентом. Оператор мобильной связи, Сервис-Провайдер и другие сторонние поставщики услуг или сайты могут устанавливать собственные условия и правила.

2.7. Банк не взимает комиссию за использование Карт в СМП.

2.8. Настоящие Условия действуют до расторжения договора по Карте.

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

2.10. Использование СМП в POS-терминалах возможно только в случае он-лайн Авторизации платежей.

2.11. Обслуживание Карты осуществляется в соответствии с Условиями использования банковских карт, а также в соответствии с законодательством РФ и правилами Платежной системы MasterCard WorldWide.

3. РЕГИСТРАЦИЯ КАРТ В СИСТЕМАХ МОБИЛЬНЫХ ПЛАТЕЖЕЙ

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

- 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. способов для дополнительной проверки Клиента Банком осуществляется Верификация Клиента и активация Токена с использованием Простой электронной подписи путём ввода Клиентом Одноразового пароля, полученного в Push-уведомлении или СМС-сообщении на номер мобильного телефона Клиента, к которому привязана услуга «Мобильный банк»;

3.4. После успешного завершения процедуры регистрации Карты в Google Pay в защищенном хранилище Мобильного устройства формируется и хранится Токен.

Токен позволяет однозначно идентифицировать Карту, используемую при совершении

платежей в СМП.

О факте успешной регистрации Карты СМП информирует Клиента посредством отправки Push-уведомления или СМС-сообщения.

3.5. Клиент может самостоятельно удалить одну или несколько Карт из СМП с помощью кнопки «Удалить».

3.6. Изображение Карты в СМП может не соответствовать реальному дизайну Карты, и содержит маскированный Номер Карты (отображены 4 последние цифры Номера Карты).

4. ПОДТВЕРЖДЕНИЕ ОПЕРАЦИИ КЛИЕНТА

4.1 Платежи в Системах мобильных платежей необходимо проводить согласно инструкциям провайдеров Google Pay.

4.2. При наличии 2 (Двух) и более Карт, зарегистрированных в СМП на одном Мобильном устройстве, в том числе других банков-эмитентов, Клиент должен выбрать Карту, с использованием которой будет совершаться платеж в СМП.

5. БЛОКИРОВКА ТОКЕНА / МОБИЛЬНОГО УСТРОЙСТВА

5.1. В случае утраты Карты Клиент обязан осуществить блокировку Карты, позвонив в Контакт-центр Банка по телефону 8 800 200 45 75.

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

5.2 В случае утраты Мобильного устройства Клиенту необходимо обратиться в Банк по телефону Контакт-центра 8 800 200 45 75 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. Клиент обязан соблюдать меры по защите информации на своем Мобильном устройстве, в частности:

- активировать функцию разблокировки экрана Мобильного устройства с использованием Пароля, Touch ID или другого безопасного метода блокировки\разблокировки Мобильного устройства;
- выбрать стойкий Пароль с общей длиной не менее 8 символов, в состав которых должны входить буквы разных регистров и цифры, если для разблокировки Мобильного устройства используется пароль;
- убедиться, что на Мобильном устройстве зарегистрированы только его биометрические данные, если для разблокировки Мобильного устройства используются биометрические данные;
- Не передавать Пароли доступа к Мобильному устройству, Одноразовые пароли, регистрационные данные Мобильного устройства, а также само Мобильное устройство третьим лицам, в том числе родственникам и знакомым;
- установить на Мобильное устройство антивирусное программное обеспечение с регулярно обновляемыми базами;
- удалить все личные данные и финансовую информацию со старого Мобильного устройства, если прекращено его использование;
- обратиться в Контакт-центр Банка по телефону 8 800 200 45 75 для блокировки ~~к~~Карты в случае подозрений на любое несанкционированное использование Мобильного устройства, а также в случае его кражи или утери;
- не блокировать любые функции безопасности, предусмотренные приложениями Мобильных устройств, для использования этих функций и процедур безопасности для защиты всех Карт, зарегистрированных в СМП;

- Не использовать Мобильные устройства, на которых получен доступ уровня root или осуществлен джейлбрейк.

7. ПРАВА И ОБЯЗАННОСТИ СТОРОН

7.1. Банк обязан:

7.1.1 Исполнять распоряжения Клиента по операциям, совершенным с использованием реквизитов Карты, в СМП;

7.1.2 принять все возможные меры к недопущению приема распоряжений с использованием реквизитов Карты в СМП 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;

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; осуществлять консультирование Клиента по вопросам регистрации Карт в СМП;

7.1.6 в целях исполнения требований законодательства информировать Клиентов о совершении каждой операции, совершенной с использованием Карты в СМП путем предоставления выписки по Карточному счету Клиента при обращении Клиента в офис Банка на бумажном носителе или при ее формировании Клиентом через Интернет-Банк, а также путем направления Push-уведомлении или СМС-сообщении на номер мобильного телефона Клиента, к которому подключена услуга «Мобильный банк»;

7.1.7 фиксировать и хранить направленные Клиенту СМС-сообщения, содержащие информацию об операциях, совершенных с использованием реквизитов Карты в СМП, не менее 3 (трех) лет;

7.1.8 обеспечить конфиденциальность информации об операциях, совершенных с использованием реквизитов Карты в СМП. При этом Банк не отвечает за конфиденциальность информации, хранящейся на Мобильном устройстве.

7.2 Банк имеет право:

7.2.1 не исполнять распоряжения Клиента, совершенные с использованием Карты в СМП в случае:

6.1.1.1 если Верификация Клиента / Верификация Карты произошла неуспешно;

6.1.1.2 если Клиентом не соблюдены требования законодательства Российской Федерации, настоящих Условий.

7.2.2 в одностороннем порядке изменять настоящие Условия, уведомив Клиента о таких изменениях не позднее, чем за 10 (Десять) календарных дней до вступления изменений в силу путем размещения указанной информации на сайте Банка в сети Интернет по адресу: www.bankdolinsk.ru ;

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

7.2.4 заблокировать, ограничить, приостановить или прекратить использование реквизитов Карты в СМП в любое время без уведомления и по любой причине, в том числе, если Клиент нарушает настоящие Условия.

7.2.5 отказать Клиенту в регистрации Карты для совершения платежей в СМП при неуспешной Верификации Клиента / Карты;

7.2.6 по своему усмотрению удалить Токен, а также удалить Карту из СМП, в том числе в случае неисполнения Клиентом п.7.3.6. настоящих Условий;

7.2.7 в любое время изменить тип банковских карт, которые могут быть использованы в СМП, или прекратить сотрудничество с тем или иным провайдером без предварительного уведомления Клиента.

7.3. Клиент обязан:

7.3.1. соблюдать настоящие Условия;

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 телефону Контакт-центра, а также путем подачи заявления в офисе Банка.

На основании уведомления 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 Кары в СМП, 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 СМС-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, выданные торговой организацией;
- иные документы и информацию, которые имеют отношение к спорной ситуации или которые могут быть затребованы Банком в рамках рассмотрения Заявления о спорной транзакции.

7.3.4. регулярно на сайте Банка www.bankdolinsk.ru отслеживать изменения,

внесенные в настоящие Условия.

7.3.5. контролировать соответствие суммы операции и текущего остатка на Карточном счете и осуществлять операции в СМП только в пределах этого остатка.

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. исполнять требования, изложенные в разделе 6 настоящих Условий.

7.4. Клиент имеет право:

7.4.1. обращаться в Банк для получения консультаций по работе в СМП.

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 СМП, а также получать информацию о результатах рассмотрения заявлений, в том числе в письменной форме.

8. ОТВЕТСТВЕННОСТЬ СТОРОН

8.1. Ответственность Клиента

Клиент несет ответственность за:

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

8.2. Ответственность Банка

8.2.1. Банк не несет ответственности:

- за работу СМП,
- за отсутствие возможности совершения в СМП операций,
- за приостановление, аннулирование или прекращение использования Карты в СМП,
- за конфиденциальность информации, хранящейся на Мобильном устройстве, в том

числе в Приложениях Google Pay.

9. ПРОЧИЕ УСЛОВИЯ

9.1. Принимая настоящие Условия, Клиент дает согласие на получение от Банка СМС-сообщений / Push-уведомлений, необходимых для совершения платежей в СМП;

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

- доступ, использование и возможность совершения платежей посредством реквизитов Карты в СМП зависит исключительно от провайдеров сервисов, а также 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.
- Банк не несет ответственности за поддержку операционной системы Мобильного устройства.