УТВЕРЖДЕНЫ

Решением Правления
Протокол от «22» января 2021 г.

и введены в действие с «22» января 2021 г.
Приказом от 22.01.2021 № 1-01-04/05

УСЛОВИЯ

использования банковских карт Банка «РЕСО Кредит» (АО) в системах мобильных платежей

Москва, 2021

СОДЕРЖАНИЕ

1. Введение

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

1.2. 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.

1.3. Настоящие Условия определяют:

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

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

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

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

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

1.5. 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.

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

1.7. Настоящие Условия действуют до расторжения договора по Карте.

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

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

1.10. Обслуживание Карты осуществляется в соответствии с Банковскими условиями проведения операций с физическими лицами в Банке «РЕСО Кредит» (АО), а также в соответствии с законодательством РФ.

1.11. Термины и определения, используемые в настоящих Условиях:

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

Банк – Банк «РЕСО Кредит» (АО), местонахождение: 119285, г. Москва, Воробьевское шоссе, дом 6, ОГРН: 1087711000046, ИНН: 7750004305, КПП: 772901001, включенный в реестр банков-участников системы обязательного страхования вкладов 10.05.2007 под № 956, регистрационный номер, присвоенный Банком России: 3450.

Банковские условия - Банковские условия проведения операций с физическими лицами в Банке «РЕСО Кредит» (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/ Apple Wallet/ Samsung 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).

Заявление - анкета о присоединении к Банковским условиям, Заявление - анкета – заполненное по форме Приложения № 3 к Банковским условиям и подписанное Клиентом заявление о присоединении к Банковским условиям, на основании которого заключается Договор (текущего) счета в рублях и иностранной валюте и/или Договор банковского вклада, и/или Договор приобретения и использования банковских карт, и/или Договор дистанционного банковского обслуживания.

Карта, Банковская карта – электронное средство платежа, эмитируемая Банком банковская карта, являющаяся средством для составления расчетных и иных документов, подлежащих оплате за счет Клиента.

Клиент – физическое лицо (резидент или нерезидент в соответствии с действующим законодательством Российской Федерации), с которым на основании Заявления-анкеты о присоединении к Банковским условиям заключен Договор приобретения и использования банковских карт, не связанное с осуществлением предпринимательской деятельности, и имеющее Мобильное устройство.

Мобильное устройство — устройство (смартфон, планшет, часы) выпускаемое корпорацией Apple Inc. с поддержкой Системы Apple Pay (список указан на сайте http://www.apple.com/apple-pay/) и/или устройство с поддержкой Системы Google Pay со следующими характеристиками: версия Android 4.4 KitKat или выше; наличие чипа NFC; на устройстве должна быть установлена официальная прошивка, заблокирован загрузчик и отключены root-права (информация представлена на https://support.google.com/pay/), Google Pay поддерживается также на смарт-часах, оснащенных бесконтактным NFC-чипом и работающих на Android Wear 2.0. и/или устройство с поддержкой Samsung Pay (список указан на сайте https://www.samsung.com/ru/support/mobile-devices/which-devices-support-samsung-pay/).

Номер Карты (FPAN) — уникальный набор цифр, наносимый на Карту, и состоящий из шестнадцати цифр.

Одноразовый пароль — комбинация символов в виде цифр, генерируемая Банком при попытке зарегистрировать Карту в Google Pay / Apple Wallet / Samsung Pay, и направляемая Клиенту в виде Push-уведомления или СМС-сообщения на указанный в Заявлении-анкете номер мобильного телефона Клиента.

Операция с использованием Банковской карты – операция, совершенная с использованием Банковской карты и/или ее реквизитов.

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.

Персональный идентификационный номер, ПИН-код, ПИН – индивидуальный код, присваиваемый Банковской карте и используемый для идентификации держателя при совершении Операций с использованием Банковской карты с помощью электронных терминалов, банкоматов и иных средств удаленного доступа к Счету СКС. 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.

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

Клиент признает, что электронный документ, сформированный для осуществления платежа посредством Системы Google Pay / Apple Pay / Samsung Pay и подписанный Простой

электронной подписью, признается равнозначным документу, подписанному собственноручной подписью.

Система ДБО – Система дистанционного банковского обслуживания (электронное средство платежа) физических лиц, позволяющая Клиенту осуществлять безналичные расчеты в форме перевода денежных средств путем передачи соответствующего распоряжения Банку, а также пользоваться иными услугами, представляемыми данным сервисом. Система дистанционного банковского обслуживания обеспечивает предоставление онлайн сервисов, формирование, прием к исполнению, хранение, обработку и исполнение ЭД в соответствии с Договором ДБО.

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

Система Apple Pay — система мобильных платежей от корпорации Apple Inc. 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 Карточного счета, используя беспроводную связь с Мобильного устройства Apple.

Система Samsung Pay – система мобильных платежей от корпорации Samsung. 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 и/или их реквизитов на мобильном устройстве с соответствующими техническими характеристиками.

Счет СКС – специальный карточный счет, открываемый Банком Клиенту на основании Договора приобретения и использования банковских карт и предусматривающий совершение Операций с использованием Банковских карт.

Токен (DPAN) — цифровое представление Карты, которое формируется по факту регистрации Карты в Google Pay / Apple Wallet / Samsung 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 / Apple Pay / Samsung Pay. Токенизация осуществляется по факту добавления Карты в СМП.

Условия – настоящие Условия использования банковских карт Банка «РЕСО Кредит» (АО) в системах мобильных платежей.

Электронный документ, ЭД – документ Клиента, сформированный в электронном виде и подписанный АСП на основании данных, введенных Клиентом в Системе ДБО, с учетом требований действующего законодательства Российской Федерации и Договора.

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).

Google Pay — официальное приложение из P1ayМаркет, установленное на устройство, работающее на платформе Android, обеспечивающее Токенизацию и хранение информации о Токенах.

Samsung Pay — официальное приложение из P1ayМаркет, предустановленное и/или устанавливаемое на устройство Samsung, работающее на платформе Android, обеспечивающее Токенизацию и хранение информации о Токенах.

Push-уведомление – информация, передаваемая Банком посредством сети Интернет на Мобильное устройство Клиента. Push-уведомления могут поступать от Банка, от Системы Google Pay / Apple Pay / Samsung Pay только при наличии доступа к сети Интернет. Push-уведомление представляет собой последовательность символов, используемых однократно.

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

2. Регистрация Карт в Системах мобильных платежей

2.1. Для осуществления расчетов через Систему Google Pay / Apple Pay / Samsung Pay Клиенту необходимо зарегистрировать в Google Pay / Apple Wallet / Samsung Pay Карту одним из способов:

- используя камеру с автоматическим заполнением Номера Карты;
- ввод Номера Карты вручную;
- иной способ при наличии технической возможности.

2.2. Для подтверждения действительности Карты осуществляется Верификации Карты с помощью CVC2 (трехзначный код, указанный на оборотной стороне Карты). Карта должна быть активна, иметь не истекший срок действия.
2.3. После ввода Номера Карты одним из указанных в п.2.1. 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 указанный в Заявлении-анкете номер мобильного телефона Клиента.
2.4. После успешного завершения процедуры регистрации Карты в Google Pay / Apple Wallet / Samsung 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.
2.5. Клиент может самостоятельно удалить одну или несколько Карт из СМП с помощью кнопки «Удалить».
2.6. Изображение Карты в СМП может не соответствовать реальному дизайну Карты, и содержит маскированный Номер Карты (отображены 4 последние цифры Номера Карты).

3. Подтверждение операции Клиента

3.1. Платежи в Системах мобильных платежей необходимо проводить согласно инструкциям провайдеров Google Pay / Apple Pay / Samsung Pay.
3.2. 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.

4. Блокировка Токена / Мобильного устройства

4.1. В случае утраты Карты Клиент обязан осуществить блокировку Карты, позвонив в Контакт-центр Банка по телефону +7 495 730-77-55. По факту блокировки Карты, блокируются все Токены для данной Карты на всех Мобильных устройствах с целью недопущения совершения расчетов в СМП.
4.2. В случае утраты Мобильного устройства Клиенту необходимо обратиться в Банк по телефону +7 495 730-77-55 с целью блокировки Токена, содержащегося на данном Мобильном устройстве. В данном случае Банк блокирует только Токен, содержащийся на данном Мобильном устройстве.

5. Требования к безопасности

5.1. 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 Банк по телефону +7 495 730-77-55 для блокировки 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.

6. Права и обязанности

6.1. Банк обязан:
6.1.1. исполнять распоряжения Клиента по операциям, совершенным с использованием реквизитов Карты, в СМП;
6.1.2. 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);
6.1.3. 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;
6.1.4. в случае неисполнения Банком своевременно и должным образом обязанности, предусмотренной п.6.1.3. 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;
6.1.5. возместить Клиенту суммы операций, которые были совершены при неуспешной Верификации Клиента; осуществлять консультирование Клиента по вопросам регистрации Карт в СМП;
6.1.6. в целях исполнения требований законодательства информировать Клиентов о совершении каждой операции, совершенной с использованием Карты в СМП путем предоставления выписки по Счету СКС Клиента при ее формировании Клиентом через Интернет-Банк, а также путем направления Push-уведомлении или СМС-сообщении на указанный в Заявлении-анкете номер мобильного телефона Клиента;
6.1.7. фиксировать и хранить направленные Клиенту СМС-сообщения, содержащие информацию об операциях, совершенных с использованием реквизитов Карты в СМП, не менее трех лет;

6.1.8. обеспечить конфиденциальность информации об операциях, совершенных с использованием реквизитов Карты в СМП. При этом Банк не отвечает за конфиденциальность информации, хранящейся на Мобильном устройстве.
6.2. Банк имеет право:
6.2.1. не исполнять распоряжения Клиента, совершенные с использованием Карты в СМП в случае:
6.2.1.1. если Верификация Клиента / Верификация Карты произошла неуспешно;
6.2.1.2. если Клиентом не соблюдены требования законодательства Российской Федерации, настоящих Условий.
6.2.2. в одностороннем порядке изменять настоящие Условия, уведомив Клиента о таких изменениях путем размещения указанной информации на официальном сайте Банка в сети Интернет;
6.2.3. в целях обеспечения безопасности устанавливать ограничения по времени действия Одноразового пароля в пределах одного сеанса соединения (тайм-аут);
6.2.4. 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;
6.2.5. отказать Клиенту в регистрации Карты для совершения платежей в СМП при неуспешной Верификации Клиента / Карты;
6.2.6. по своему усмотрению удалить Токен, а также удалить Карту из СМП, в том числе в случае неисполнения Клиентом требований настоящих Условий;
6.2.7. 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.
6.3. Клиент обязан:
6.3.1. соблюдать настоящие Условия;
6.3.2. 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 +7 495 730-77-55, а также путем подачи заявления в офисе Банка. На основании уведомления Банк в срок, указанный в п. 6.1.3. 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;
6.3.3. 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;
6.3.4. регулярно на официальном сайте Банка отслеживать изменения, внесенные в настоящие Условия;
6.3.5. контролировать соответствие суммы операции и текущего остатка на Счете СКС и осуществлять операции в СМП только в пределах этого остатка.

6.3.6. 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.
6.3.7. исполнять требования, изложенные в разделе 5 настоящих Условий.
6.4. Клиент имеет право:
6.4.1. обращаться в Банк для получения консультаций по работе в СМП;
6.4.2. 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;
6.4.3. 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.

7. Ответственность сторон

7.1. Ответственность Клиента.
7.1.1. Клиент несет ответственность за:
- сохранение конфиденциальности Пароля и других средств Верификации Клиента;
- использование Мобильного устройства третьими лицами;
- за операции, совершенные Клиентом в СМП с использованием реквизитов Карты, зарегистрированной в СМП на Мобильном устройстве Клиента;
- нарушение требований к технической защите Мобильного устройства, указанных в разделе 5 настоящих Условий.

7.2. Ответственность Банка.
7.2.1. 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 / Apple Wallet / Samsung Pay.

8. Прочие условия

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