а) банк

банк
александровский

Условия использования банковских карт ПАО Банк «АЛЕКСАНДРОВСКИЙ» в Системах мобильных платежей

Санкт-Петербург
2019

Оглавление

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 3
2. ОБЩИЕ ПОЛОЖЕНИЯ 5
3. РЕГИСТРАЦИЯ КАРТ В СИСТЕМАХ МОБИЛЬНЫХ ПЛАТЕЖЕЙ 6
4. ПОДТВЕРЖДЕНИЕ ОПЕРАЦИИ КЛИЕНТА 6
5. БЛОКИРОВКА ТОКЕНА / МОБИЛЬНОГО УСТРОЙСТВА 6
6. ТРЕБОВАНИЯ К БЕЗОПАСНОСТИ 7
7. ПРАВА И ОБЯЗАННОСТИ СТОРОН 7
8. ОТВЕТСТВЕННОСТЬ СТОРОН 9

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Apple ID/ Google ID/Samsung 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 – ПАО Банк «АЛЕКСАНДРОВСКИЙ».

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

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

При регистрации Клиента в Apple Wallet/Google Pay/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).

Карта – выпущенная Банком платежная карта международной платежной системы VISA International или MasterCard Worldwide, являющаяся электронным средством для осуществления безналичных расчетов, предназначенным для оплаты товаров работ и услуг, а также получения денежных средств и выполнения других операций, в соответствии с Договором комплексного банковского обслуживания на территории РФ и за ее пределами. В рамках настоящих Условий под понятие «Карта» попадают только карты VISA Gold, VISA Infinite, MasterCard Gold, MasterCard Business.

Клиент – физическое лицо, являющееся держателем Карты, 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/)/устройство с поддержкой Системы Google Pay со следующими характеристиками: версия Android 4.4 KitKat или выше; наличие чипа NFC; устройство Samsung с отключённым сервисом Knox; на устройстве должна быть установлена официальная прошивка, заблокирован загрузчик и отключены root-права (список указан на сайте https://pay.google.com/intl/ru_ru/about/)/устройство Samsung Galaxy или Samsung Gear (список указан на сайте https://www.samsung.com/ru/apps/mobile/samsungpay)

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

Одноразовый пароль – комбинация символов в виде цифр, генерируемая Банком при попытке зарегистрировать Карту в Apple Wallet/ Google Pay/Samsung Pay, и направляемая Клиенту в виде СМС-сообщения на номер мобильного телефона Клиента, указанный Клиентом в Заявлении на выпуск карты.

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.

Правила - Правила комплексного обслуживания физических лиц в ПАО Банк «АЛЕКСАНДРОВСКИЙ».

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

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

Система Apple Pay – система мобильных платежей от корпорации Apple Inc. Система Apple Pay совместима с существующими бесконтактными считывателями. 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 Карточного счета, используя беспроводную связь с Мобильного устройства Apple. Использование Системы Apple Pay осуществляется в соответствии с настоящими Условиями, Условиями по Карте и Тарифами.

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

Система Samsung Pay – система мобильных платежей от компании Samsung, которая использует комбинацию технологии NFC (Near Field Communication) и MST (Magnetic Secure Transmission). Технология MST работает по принципу создания динамически меняющегося магнитного поля для передачи на платежный терминал данных, аналогичных данным магнитной полосы банковской карты, когда владелец смартфона и карты инициирует оплату через Samsung Pay. Эта технология позволяет превратить любой платежный терминал (исключение составляют платежные терминалы, на которых недоступен внешний магнитный считыватель) в средство бесконтактной оплаты. Сервис Samsung Pay использует встроенную систему безопасности смартфона – Samsung KNOX, токенизацию и двухфакторную авторизацию для защиты платежных данных. Для совершения платежа необходимо авторизоваться при помощи отпечатка пальца или пароля приложения.

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.

Тарифы – установленные Банком тарифы комиссионного вознаграждения за обслуживание клиентов – физических лиц, размещенные на Сайте Банка и в ВСП Банка. Тарифы Банка – документ, регламентирующий стоимость услуг, предоставляемых Банком Клиентам.

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

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 PlayМаркет, установленное на устройство, работающее на платформе Android, обеспечивающее Токенизацию и хранение информации о Токенах.

Samsung Pay – приложение на смартфонах Samsung Galaxy и устройствах Samsung Gear, обеспечивающее хранение информации о карте при оплате посредством сервиса Samsung Pay.

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

Touch ID — дактилоскопический датчик/сканер Отпечатков пальцев. Touch ID позволяет Клиентам использовать Отпечаток пальца в качестве подтверждения покупки в App Store, iTunes Store и iBooks Store.

2. ОБЩИЕ ПОЛОЖЕНИЯ

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

2.2 Настоящие условия являются соглашением между держателем Карты и Банком, частью Договора комплексного банковского обслуживания. 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.

2.3 Настоящие Условия определяют:

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

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

2.5 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.

2.6 Банк не взимает комиссию за использование Карт в СМП.

2.7 Настоящие Условия действуют до закрытия Карты.

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

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

2.10 Обслуживание Карты осуществляется в соответствии с Правилами комплексного обслуживания физических лиц в ПАО Банк «АЛЕКСАНДРОВСКИЙ», Руководством пользователя по работе с картами международных платежных систем Visa International и Mastercard Worldwide, а также в соответствии с законодательством РФ и правилами Платежной системы Visa International.

2.11 Принимая настоящие Условия, Клиент дает согласие на получение от Банка SMS-сообщений, необходимых для совершения платежей в СМП.

3. РЕГИСТРАЦИЯ КАРТ В СИСТЕМАХ МОБИЛЬНЫХ ПЛАТЕЖЕЙ

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

- используя камеру 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 CVV2. 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 СМС-сообщении на номер мобильного телефона Клиента, которому привязана услуга «СМС-сервис» или который указан в Заявлении на оформление карты.

3.4. После успешного завершения процедуры регистрации Карты в Apple Wallet/ Google Pay/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 СМС-сообщения или Push-уведомления.

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 Apple Pay, Google Pay и Samsung 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 8 800 222-87-07.

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 8 800 222-87-07 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 биометрические данные Клиента, 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 8 800 222-87-07 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.

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;

7.1.6. осуществлять консультирование Клиента по вопросам регистрации Карт в СМП;

7.1.7. 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 СМС-сообщении на номер мобильного телефона Клиента, к которому подключена услуга «СМС-сервис»;

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

7.1.9. 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:

- если Верификация Клиента / Верификация Карты произошла неуспешно;
- 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 www.alexbank.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-центр Банка 8 800 222-87-07, 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 SMS-сообщения 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.alexbank.ru отслеживать изменения, внесенные в настоящие Условия;

7.3.5. контролировать соответствие суммы операции и текущего остатка на счете Карты 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 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;

7.4.4. удалить зарегистрированную Карту из СМП.

8. ОТВЕТСТВЕННОСТЬ СТОРОН

8.1. Ответственность Клиента.

8.1.1. 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 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 управляет СМП или сетями беспроводной связи и не имеет контроля над их управлением.

8.2.2. Банк не несет ответственности:

- перед пользователями прямо или косвенно за любые обстоятельства, при которых прерывается или нарушается функционирование СМП, например, недоступность Системы мобильных платежей или услуг беспроводной связи, коммуникационных услуг, задержки в сети, перебои в работе системы или прерывание беспроводного соединения;
- за СМП или какие-либо услуги беспроводной связи, используемые для доступа, использования или поддержания таких услуг;
- за работу мобильного устройства пользователя, а также не предоставляет никаких заверений или гарантий по отношению к вышеупомянутому;
- если иное не предусмотрено законом, ни при каких обстоятельствах банк не несет ответственности за любые понесенные убытки, связанные с использованием или невозможностью использования СМП, вне зависимости от причин и оснований возникновения ответственности;
- за конфиденциальность информации, хранящейся на Мобильном устройстве, в том числе в Приложениях Apple Wallet/ Google Pay/Samsung Pay.

8.2.3. Банк не гарантирует доступность Системы мобильных платежей для проведения операции, наличие возможности совершения операций в том или ином торговом предприятии или непрерывное либо безошибочное использование Системы мобильных платежей. Использование Системы мобильных платежей включает в себя передачу информации о пользователе в электронном виде по предоставленным третьими лицами каналам связи.