

Правила и условия использования Карт в Платежных мобильных сервисах

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила и условия использования Карт в Платежных мобильных сервисах (далее по тексту – Правила) являются дополнением и неотъемлемой частью Условия выпуска, обслуживания и использования банковских карт, эмитированных ООО «АТБ» Банк (приложение № 1 к Договору комплексного банковского обслуживания физических лиц в ООО «АТБ» Банк, далее - Условия).

1.2. Клиент подтверждает согласие и присоединение к Правилам в процессе регистрации Держателем карты Карты/Дополнительной карты в Платежном мобильном сервисе и создании Карточного токена. Клиент считается вступившим в договорные отношения с Банком в части проведения операций с использованием Карточного токена с даты создания Карточного токена.

1.3. Термины, используемые в Правилах, написанные с заглавной буквы, имеют то же значение, что и в Условиях, если иное не установлено Правилами. В случае разночтений термины Правил имеют преимущественную силу.

1.4. В случае противоречий между Правилами и Условиями, положения Правил имеют преимущественную силу.

1.5. Если иное прямо не установлено Условиями и Правилами, то под термином «Операция» в Условиях понимаются, в том числе, Операции с использованием Карточного токена. Все положения Условия распространяются на Операции с использованием Карточного токена, если иное прямо не установлено Условиями и Правилами.

1.6. При совершении Операции с использованием Карточного токена порядок расчетов, изложенный в Условиях, не изменяется.

1.7. При использовании Карточного токена условия обслуживания Карты (установленные лимиты, ограничения на Карте, тарифы, участие Карты в программах лояльности) не изменяются, комиссии за осуществление операций подлежат уплате в случаях, предусмотренных ДКБО и Тарифами.

1.8. Дополнительная информация о порядке и способах создания и использования Карточного токена в различных Платежных мобильных сервисах размещена в информационно-телекоммуникационной сети «Интернет» на сайте Банка по адресу www.avtotorgbank.ru.

2. ДОПОЛНИТЕЛЬНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Аутентификационные данные - пароль Клиента для авторизации в Платежном мобильном сервисе (включая, но не ограничиваясь биометрические данные (авторизация по отпечатку пальца, биометрии лица), установленный в соответствии с правилами Организации, ПИН-код, а также другие данные, используемые для доступа в Платежный мобильный сервис и проведения Операции с использованием Карточного токена).

2.2. Карточный токен – виртуальное представление Карты в Платежном мобильном сервисе, содержащее специальный цифровой код – Токен, соответствующий конкретной Карте и хранящийся в Платежном мобильном сервисе, используемый при проведении Операции с использованием Карточного токена.

2.3. Мобильное устройство – смартфон, мобильный телефон (телефон сотовой связи), поддерживающий технологию Java™ MIDP 2.0., либо дополненный функциональностью

карманного персонального компьютера или планшетный компьютер, либо иное устройство, совместимое с Платежным мобильным сервисом.

2.4. Операция с использованием Карточного токена - способ совершения Операции с использованием Карточного токена путем близкого поднесения или прикосновения Мобильного устройства, поддерживающего Платежный мобильный сервис, к считывающему платежному терминалу без физического контакта с указанным терминалом или способ совершения Операции на сайте ТСП через сеть Интернет или посредством мобильного приложения ТСП с использованием Платежного мобильного сервиса.

2.5. Платежный мобильный сервис – сервис (Mir Pay¹ (мобильное приложение платежной системы «Мир»), Samsung Pay, предоставляемый сторонними некредитными (в том числе иностранными) организациями (далее – Организация), позволяющий использовать Мобильное устройство для проведения Операции с использованием Карточного токена.

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

2.7. Одноразовый пароль – комбинация символов в виде 6-ти цифр, генерируемая МПС при попытке зарегистрировать Карту, и направляемая Клиенту в виде СМС-сообщения от Банка на номер мобильного телефона Клиента, зафиксированный в информационных системах Банка.

2.8. Биометрические данные – однозначное цифровое представление биометрических данных Клиента – владельца Мобильного устройства (таких, как рисунок кожи на пальце руки Клиента, радужек глаз Клиента и прочих, при условии возможности использовать такие данные на Мобильном устройстве и в Мобильном платежном приложении). Биометрические данные настраиваются Клиентом на Мобильном устройстве и обеспечивают однозначную Верификацию Клиента.

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

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

2.11. 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.

2.12. Простая электронная подпись – электронная подпись, которая посредством использования Одноразового пароля /Пароля /Биометрических данных, подтверждает факт совершения определённого действия Клиентом в Системе (платеж в Системе, регистрация Карты). Клиент признает, что электронный документ, сформированный для осуществления платежа посредством Системы и подписанный Простой электронной подписью, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью.

2.13. Система - Mir Pay /Samsung Pay.

2.14. Счет карты – банковский счет, открытый Банком на имя Клиента, и предназначенный для проведения расчетов с использованием Карты или ее реквизитов. Счет карты является текущим счетом и предназначен для проведения расчетов с использованием Карты или ее

¹ Сервис доступен Держателям карт платежной системы «МИР» с момента технической реализации.

реквизитов, не связанных с осуществлением предпринимательской деятельности или частной практики.

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

2.16. Токенизация – процесс замены Номера Карты (FPAN) на Токен (DPAN), позволяющий однозначно определить Карту, использованную для совершения операций с использованием Системы.

2.17. NFC (Near Field Communications) - технология высококачественной беспроводной связи с малым радиусом действия, которая позволяет производить бесконтактный обмен данными между Мобильным устройством и устройством POS-терминала.

2.18. MST (Magnetic Secure Transmissions) – собственная технология Samsung, используемая в Системе Samsung Pay, позволяющая Мобильным устройствам Samsung с поддержкой MST использовать переменное магнитное поле для передачи данных на POS-терминал.

3. СОЗДАНИЕ И ИСПОЛЬЗОВАНИЕ КАРТОЧНОГО ТОКЕНА В ПЛАТЕЖНОМ МОБИЛЬНОМ СЕРВИСЕ

3.1. Карточный токен может быть создан к любой активированной и не заблокированной Карте.

3.2. Банк предоставляет Держателям карт возможность инициировать создание Карточного токена посредством Платежного мобильного сервиса. Держатель карты регистрирует Карту в Платежном мобильном сервисе путем ввода реквизитов Карты в Платежном мобильном сервисе в порядке, определенном Организацией, предоставляющей соответствующий Платежный мобильный сервис.

3.3. В процессе регистрации, проводимой Держателем Карты в соответствии с пунктом 3.2 Правил, Банк направляет на Доверенный номер Держателю карты SMS-сообщение с Одноразовым паролем.

3.4. Карточный токен считается созданным Держателем карты, если отправленный Банком Одноразовый пароль совпадает с введенным Держателем карты в Платежном мобильном сервисе Одноразовым паролем, при условии, что время ввода Одноразового пароля не истекло. При этом Клиент поручает Банку передать в организацию, предоставляющую Платежный мобильный сервис, всю информацию, необходимую для создания Карточного токена.

3.5. Банк подтверждает возможность использования Карточного токена направлением Держателю Карты соответствующего SMS-сообщения/Push-уведомления на Доверенный номер.

3.6. Обязательным условием для создания Карточного токена является наличие в Банке актуальной информации о Доверенном номере, на который Банком отправляется Одноразовый пароль.

3.7. Для одной Карты возможно создание нескольких Карточных токенов – для каждого из Мобильных устройств, в том числе для наручных часов или иных устройств, поддерживающих Платежный мобильный сервис.

3.8. Банк, Платежная система или сторонняя организация, предоставляющая Платежный мобильный сервис, могут устанавливать ограничение на максимальное количество Карточных токенов, создаваемых к одной Карте, а также отказать в создании Карточного токена без объяснения причин.

3.9. Хранение Карточных токенов, порядок их использования, удаление в Платежном мобильном сервисе осуществляется в соответствии с условиями пользовательского соглашения, заключенного между Держателем карты и Организацией.

3.10. Установка Платежного мобильного сервиса производится Держателем карты самостоятельно на Мобильное устройство, принадлежащее непосредственно самому Держателю карты, соответственно.

3.11. Проведение Операции с использованием Карточного токена посредством Платежного мобильного сервиса без ввода пароля/отпечатка пальца руки/Биометрических данных Держателя карты возможно в случае, если это предусмотрено в пользовательском соглашении, заключаемом между Держателем карты и Организацией, либо допускается условиями использования Платежного мобильного сервиса. В этом случае безусловным подтверждением совершения Держателем карты Операции с использованием Карточного токена является физическое присутствие Карточного токена в момент совершения операции.

3.12. С информацией о наличии или отсутствии дополнительных ограничений применения Платежного мобильного сервиса, о случаях приостановления или прекращения применения Платежного мобильного сервиса со стороны Организации, а также с информацией об установлении, изменении размера и/или порядка взимания с Держателя карты вознаграждения за применение Платежного мобильного сервиса Организацией Держатель Карты может ознакомиться в пользовательском соглашении, заключенном между Держателем Карты и Организацией, на официальном сайте такой организации в сети Интернет или путем обращения в такую Организацию.

3.13. При блокировании Карты Банком по любой причине осуществляется блокировка Карточного токена. Держатель карты также может самостоятельно, по своему желанию, осуществлять блокировку Карточного токена по Карте. Осуществить блокировку (приостановить совершение операций с использованием Карточного токена)/разблокировку Карточного токена (возобновить совершение операций с использованием Карточного токена) Держатель карты может через Службу поддержки клиентов.

3.14. Блокировка/удаление Карточного токена не влечет за собой автоматическую блокировку Карты.

3.15. В случае обнаружения Утраты Мобильного устройства на котором был зарегистрирован Карточный токен, и/или использования Карточного токена (в том числе в случае подозрений о возможности возникновения подобных ситуаций) без согласия Держателя Карты, Держатель Карты обязан незамедлительно сообщить об этом в Банк для приостановления совершения операций с использованием Карточного токена в порядке и сроки, определенные Условиями.

4. ПРАВА И ОБЯЗАННОСТИ БАНКА

4.1. БАНК ОБЯЗУЕТСЯ:

4.1.1. Доводить до сведения Держателей карты справочную информацию по вопросам использования Карточного токена:

- путем размещения актуальной информации на Сайте Банка;
- через Службу поддержки клиентов;
- в Подразделениях Банка.

4.2. БАНК ИМЕЕТ ПРАВО:

4.2.1. Отказать в создании Карточного токена к Карте, по своему усмотрению и без объяснения причин.

4.2.2. Прекратить действие Карточного токена, в следующих случаях:

- в случае возникновения подозрений о неправомерном использовании Карты и/или Карточного токена и невозможности получить от Держателя Карты подтверждение правомерности проведения Операции любым способом, в том числе с использованием Доверенного номера;
- в случае обнаружения Банком незаконных Операций с использованием Карты;

- в случае предоставления Платежной системой информации о незаконном использовании Карты;
 - в случае нарушения Держателем карты ДКБО;
 - в случае закрытия Карты или Счета карты Банком в соответствии с Условиями;
 - в иных случаях, установленных Условиями.
- 4.2.3. Прекратить предоставление услуг через Мобильные платежные сервисы в случае отказа поставщиков Мобильных сервисов в предоставлении услуг.

5. ПРАВА И ОБЯЗАННОСТИ ДЕРЖАТЕЛЯ КАРТЫ

5.1. ДЕРЖАТЕЛЬ КАРТЫ ОБЯЗУЕТСЯ:

- 5.1.1. До инициирования создания Карточного токена ознакомиться с условиями создания и использования Карточного токена согласно условиям пользовательского соглашения, заключенного между Держателем карты и Организацией, а также с информацией, размещенной на Сайте Банка.
- 5.1.2. Инициировать создание Карточных токенов в Платежном мобильном сервисе только для Карт, выпущенных на имя самого Держателя карты.
- 5.1.3. Производить установку Платежного мобильного сервиса самостоятельно на Мобильное устройство, принадлежащее непосредственно самому Держателю Карты.
- 5.1.4. Соблюдать и исполнять Правила, а также при наличии Дополнительной карты обеспечить соблюдение и исполнение Правил Держателем Дополнительной карты.
- 5.1.5. Обеспечить конфиденциальность Аутентификационные данные, а также сохранность Мобильного устройства таким же образом, как обеспечивается сохранность банковской Карты и ПИН-кода.

5.2. ДЕРЖАТЕЛЬ КАРТЫ ИМЕЕТ ПРАВО:

- 5.2.1. В любое время отказаться от использования Карточного токена, удалив его посредством Платежного мобильного сервиса.
- 5.2.2. В любое время заблокировать использование Карточного токена через Службу поддержки клиентов.
- 5.2.3. В случае блокировки Карточного токена Клиент дает разрешение Банку продолжать обработку Операций с использованием Карточного токена, совершенных до момента блокировки Карточного токена.

6. КОНФИДЕНЦИАЛЬНОСТЬ И БЕЗОПАСНОСТЬ

- 6.1. Держатель карты ознакомлен и соглашается, что Банк вправе осуществлять сбор, обработку и использование технических, личных данных и связанной с ними информации, включая, но не ограничиваясь, о Мобильном устройстве Держателя карты, чтобы обеспечивать:
- обновление и усовершенствование продуктов, услуг Банка;
 - повышения безопасности оказываемых услуг;
 - предотвращения мошенничества.
- 6.2. Банк не несет ответственности за услуги, предоставляемые Организацией. Таким образом, любая информация, которую собирает Организация при использовании Держателем карты Карточного токена, регулируется пользовательским соглашением, заключенным между Держателем карты и Организацией, и не регулируется настоящими Правилами, а также Условиями и ДКБО.
- 6.3. В случае потери или кражи Мобильного устройства, компрометации Карточного токена, компрометации Аутентификационных данных, использования Платежного мобильного сервиса без согласия Держателя карты, Держатель карты обязан незамедлительно после обнаружения указанных фактов, но не позднее дня, следующего за днем получения

уведомления от Банка о совершенной операции, уведомить Банк в порядке, определенном Условиями.

6.4. Держатель карты обязан оказывать содействие Банку при проведении любых расследований и использовать меры для предотвращения мошенничества или иные меры, которые могут предотвратить компрометацию Карт, Карточных токенов, Аутентификационных данных.

6.5. В Платежном мобильном сервисе могут использоваться определенные функции и применяться меры обеспечения безопасности для защиты от несанкционированного использования. Ответственность за такие функции и процедуры несет Организация. Клиент обязуется не отключать такие функции и использовать указанные функции и меры безопасности для обеспечения защиты.

6.6. Клиент соглашается с тем, что Банк не несет ответственности перед Клиентом и/или Держателем карты и/или третьей стороной:

- в случае блокировки, ограничения, приостановления или прекращения Организацией использования Держателем карты Карточного токена и/или изменения Организацией функций Платежного мобильного сервиса;
- за любые обстоятельства, которые могут прервать, создать препятствия или иным образом отразиться на функционировании Карточного токена, включая недоступность услуг Платежного мобильного сервиса или услуг беспроводной связи, коммуникаций, задержек сети, ограничений беспроводного покрытия, сбоев системы или прерывание беспроводной связи;
- за нарушение конфиденциальности и безопасности электронной передачи данных, реализуемой через соединения третьей стороной;
- при нарушении Держателем карты Правил;
- при потере или краже Мобильного устройства, компрометации Мобильного устройства по вине Держателя карты (в том числе при проведении настроек оператором беспроводной связи);
- при компрометации Держателем карты Аутентификационных данных, Карточного токена.

6.7. Настоящие Правила являются дополнительными и должны читаться одновременно с Условиями.

6.8. Держатель карты соглашается с тем, что Банк не консультирует по вопросам, не относящимся к его компетенции, а именно, включая, но не ограничиваясь:

- по вопросам, связанным с поддержкой Мобильных устройств, разрешенных для использования в Платежном мобильном сервисе;
- по вопросам предоставления сведений о конфиденциальности и безопасности использования Мобильного устройства, Платежного мобильного сервиса, сети Интернет;
- по вопросам установленных ограничений и лимитов в отношении услуг Платежного мобильного сервиса, а также минимальным требованиям по программному и аппаратному обеспечению Мобильных устройств.