Приложение

УТВЕРЖДЕНЫ
приказом АО АКБ «МЕЖДУНАРОДНЫЙ
ФИНАНСОВЫЙ КЛУБ» от 21.10.2020 № 233

УСЛОВИЯ
ИСПОЛЬЗОВАНИЯ РАСЧЕТНЫХ БАНКОВСКИХ КАРТ АО АКБ «МЕЖДУНАРОДНЫЙ ФИНАНСОВЫЙ КЛУБ» В СИСТЕМАХ МОБИЛЬНЫХ ПЛАТЕЖЕЙ

Москва, 2020

ОГЛАВЛЕНИЕ

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.1 **Банк** – АКЦИОНЕРНОЕ ОБЩЕСТВО АКЦИОНЕРНЫЙ КОММЕРЧЕСКИЙ БАНК «МЕЖДУНАРОДНЫЙ ФИНАНСОВЫЙ КЛУБ».

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

1.3 **Верификация Клиента** - процедура подтверждения полномочий Клиента для предоставления прав доступа.

При регистрации Клиента в Apple Wallet / 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 с использованием технологий Touch ID / Face ID / биометрических систем аутентификации и/или дополнительным вводом ПИН-кода Карты/ПИН-кодом приложения (при платежах через Электронный терминал).

1.4 **Договор** - Договор о выдаче и использовании расчетной банковской карт, заключенный между Клиентом и Банком.

1.5 **Карта –** выпущенная Банком платежная карта международной платежной системы Visa Int., являющаяся электронным средством платежа для осуществления безналичных расчетов, предназначенным для оплаты товаров работ и услуг, а также получения денежных средств и выполнения других операций на территории РФ и за ее пределами.

1.6 **Специальный карточный счет, специальные карточные счета в случае выпуска Мультивалютной Карты (СКС)** - банковский счет, открываемый на имя Клиента для отражения операций с использованием Карты/ Реквизитов Карты / Токена, не связанных с осуществлением предпринимательской деятельности или частной практики.

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

1.8 **Мобильное устройство –** устройство (смартфон, планшет, часы) выпускаемое корпорацией Apple Inc. с поддержкой Системы Apple Pay / устройство с поддержкой Системы Google Pay со следующими характеристиками: версия Android 4.4 или выше; наличие чипа NFC; на устройстве должна быть установлена официальная прошивка, заблокирован загрузчик и отключены root-права.

1.9 **Одноразовый пароль –** комбинация символов в виде 6-ти цифр, генерируемая Банком при регистрации Карты в Apple Wallet / Google Pay, и направляемая Клиенту в виде SMS-сообщения на Номер мобильного телефона Клиента, к которому подключена услуга «SMS- информирования».

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

1.11 **ПИН-код - Персональный идентификационный номер (ПИН-код)** - секретный цифровой код, являющийся аналогом собственноручной подписи Клиента, устанавливаемый для совершения операций с использованием Карты /Реквизитов Карты / Токена. ПИН-код генерируется с соблюдением конфиденциальности и не подлежит разглашению третьим лицам. Ввод ПИН-кода при совершении операции с использованием Карты является для Банка подтверждением факта совершения операции Клиентом.

1.12 **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.

1.13 **Правила** - Правила выдачи и использования расчетных банковских карт АО АКБ «МЕЖДУНАРОДНЫЙ ФИНАНСОВЫЙ КЛУБ», размещенные на Официальном сайте Банка.

1.14 **Простая электронная подпись –** электронная подпись, которая посредством использования Одноразового пароля / Пароля / Отпечатка пальца / математического образа отсканированного лица / результатов полученных при использовании иных биометрических систем аутентификации, подтверждает факт совершения определённого действия Клиентом в Системе Apple Pay/ Google Pay (платеж в Системе Apple Pay / Google Pay, регистрация Карты в Apple Wallet / Google Pay).

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

1.15 **Система Apple Pay** – система мобильных платежей от корпорации Apple Inc, позволяющая производить оплату 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 приложением Apple Wallet. Для подтверждения платежа используется Touch ID и/или Face ID и/или Пароль. Система Apple Pay совместима с существующими бесконтактными считывателями Visa PayWave и 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.

1.16 **Система Google Pay** - система мобильных платежей от корпорации Google, работающих под операционной системой Android, позволяющая производить оплату при помощи беспроводной связи Мобильного устройства, работающего под управлением операционной системы Android, без физического использования Карты. С помощью Системы Google Pay владельцы Мобильных устройств, работающих под управлением операционной системы Android, могут оплачивать покупки по технологии NFC («ближняя бесконтактная связь») в сочетании с приложением Google Pay. Google Pay использует возможности биометрических систем аутентификации, таких как сканер Отпечатка пальца и сканер радужки глаза (в случаях когда это возможно), которые обеспечивают однозначную Верификацию Клиента в Мобильном устройстве.

1.17 **Система мобильных платежей (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 Карт на мобильном устройстве с соответствующими техническими характеристиками.
Использование СМП осуществляется в соответствии с настоящими Условиями использования расчетных банковских карт АО АКБ «МЕЖДУНАРОДНЫЙ ФИНАНСОВЫЙ КЛУБ» и Договором о выдаче и использовании расчетной банковской карты.

1.18 **Токен** – цифровое представление Карты, которое формируется по факту регистрации Карты в Apple Wallet / Google Pay, и которое хранится в зашифрованном виде в защищенном хранилище Мобильного устройства.

1.19 **Токенизация –** процесс создания Токена и его связки с Реквизитами карты, позволяющий однозначно определить Карту, зарегистрированную для совершения операций с использованием Системы Apple Pay / Google Pay. Осуществляется по факту добавления Карты в СМП.

1.20 **Условия -** настоящие Условия использования расчетных банковских карт АО АКБ «МЕЖДУНАРОДНЫЙ ФИНАНСОВЫЙ КЛУБ».

1.21 **Apple Wallet** — предустановленное на Мобильном устройстве Apple приложение, позволяющее осуществить Токенизацию и хранить информацию о Токенах, а также информацию, позволяющую однозначно различить ту или иную Карту: изображение Карты, последние 4 цифры номера Карты.

1.22 **Face ID** - сканер объёмно-пространственной формы лица человека, обеспечивает однозначную Верификацию Клиента в Мобильном устройстве.

1.23 **Google Pay –** приложение, работающее на платформе Android, обеспечивающее Токенизацию и хранение информации о Токенах.

1.24 **Touch ID —** сканер Отпечатков пальцев, обеспечивает однозначную Верификацию Клиента в Мобильном устройстве.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1 Настоящие Условия определяют порядок оказания Банком Клиенту услуг по проведению расчетов по операциям, совершенным с использованием Токенов в СМП.

2.2 В случае регистрации Клиентом карты в СМП настоящие Условия являются соглашением между Клиентом 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.

2.3 Информация из аппаратно-программного комплекса платежной системы / процессинговой компании / Банка может использоваться в качестве доказательств при рассмотрении споров, в том числе в судебном порядке.

2.4 Настоящие Условия определяют:

- процесс регистрации Карты в СМП, при котором Клиент принимает настоящие Условия полностью;
- порядок совершения и подтверждения операции, совершенной Клиентом в СМП;
- 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.

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. Тем не менее, провайдеры, а также иные сторонние организации, в том числе операторы беспроводной связи или поставщики услуг передачи данных могут взимать плату за услуги в связи с использованием Мобильного устройства или системы Мобильного устройства или СМП. При этом все комиссии и другие платежи применимые к Клиенту в соответствии с условиями заключенных договоров, так же применяются ко всем операциям, совершенным с использованием СМП.

2.8 Банк, а также СМП или торгово-сервисные предприятия по своему усмотрению могут устанавливать лимиты на совершение операций покупки.

2.9 Настоящие Условия действуют до расторжения Договора.

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

2.11 Использование СМП в Электронных терминалах возможно только в случае Авторизации платежей в режиме реального времени (он-лайн Авторизации).

2.12 Обслуживание Карты осуществляется в соответствии с Договором, законодательством Российской Федерации и правилами платежной системы Visa Int.

2.13 В рамках настоящих Условий используются термины, определения и сокращения, приведенные в разделе 1 или специально указанные в тексте Условий. Иные используемые термины и определения применяются в их значениях, приведенных в Правилах выдачи и использования расчетных банковских карт АО АКБ «МЕЖДУНАРОДНЫЙ ФИНАНСОВЫЙ КЛУБ» (Правилах), размещенных на Официальном сайте Банка, а также в значениях, установленных актами законодательства Российской Федерации и нормативно-правовыми актами Банка России.

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

2.15 Настоящие Условия составлены на русском языке. В случае перевода текста настоящих Условий на любой другой язык, текст на русском языке будет иметь преимущественную силу.

3. РЕГИСТРАЦИЯ КАРТ В СИСТЕМАХ МОБИЛЬНЫХ ПЛАТЕЖЕЙ

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

- методом распознавания/считывания информации, нанесенной на Карту;
- вводом Реквизитов Карты вручную;
- иным способом при наличии технической возможности.

Карта должна быть активна, иметь не истекший срок действия. Для подтверждения действительности Карты осуществляется Верификация Карты.

3.2 После регистрации Карты осуществляется Верификация Клиента путём ввода Клиентом Одноразового пароля, полученного в SMS-сообщении на Номер мобильного телефона Клиента.

После успешного завершения процедуры регистрации/Верификации Карты и Верификации Клиента в Apple Wallet / Google Pay в защищенном хранилище Мобильного устройства формируется и хранится Токен. Активация Токена осуществляется использованием Простой электронной подписи. Об активации Токена в СМП Банк информирует Клиента посредством отправки SMS-сообщения на Номер мобильного телефона Клиента.

3.3 Токен позволяет однозначно идентифицировать Карту, используемую при совершении платежей в СМП.
3.4 Клиент может самостоятельно удалить одну или несколько Карт из СМП с помощью функциональности соответствующего приложения Apple Wallet или Google Pay.
3.5 Изображение Карты в СМП может не соответствовать реальному дизайну Карты, и содержит маскированный Номер Карты (отображены четыре последние цифры номера карты).

4. ПОДТВЕРЖДЕНИЕ ОПЕРАЦИИ КЛИЕНТА

4.1 Платежи в СМП необходимо проводить согласно инструкциям провайдеров Apple Pay / Google Pay.
4.2 При наличии 2 (Двух) и более Карт, зарегистрированных в СМП на одном Мобильном устройстве, в том числе других эмитентов, Клиент должен выбрать Карту, с использованием которой будет совершаться платеж в СМП.

5. БЛОКИРОВКА КАРТЫ / ТОКЕНА

5.1 В случае утраты Карты Клиент обязан осуществить Блокировку Карты одним из следующих способов:

- обратившись в службу круглосуточной клиентской поддержки процессингового центра по телефону +7 (495) 23-23-7-23;
- при наличии заключенного с Банком договора и доступа в Систему ДБО «МФК-Онлайн» выполнить необходимые действия блокировке карты в Системе ДБО «МФК-Онлайн»;
- обратившись лично в подразделение Банка;
- обратившись в Банк по телефонам +7 (495) 644-35-84, +7 (495) 287-02-60, в период с понедельника по четверг с 9.00 до 18.00 МСК, в пятницу с 9.00 до 16.45 МСК, в Рабочие предпраздничные дни режим работы сокращен на 1 час

По факту Блокировки Карты, блокируется возможность совершения операций с использованием Токенов для данной Карты на всех Мобильных устройствах с целью недопущения совершения расчетов в СМП.

5.2 В случае утраты или кражи Мобильного устройства, а также в случае, когда учетные данные для доступа к Мобильному устройству скомпрометированы и/или стали доступны третьим лицам Клиенту необходимо обратиться с целью деактивации Токена Карты Банка, содержащегося на данном Мобильном устройстве:

- в Банк по телефонам +7 (495) 644-35-84, +7 (495) 287-02-60, в период с понедельника по четверг с 9.00 до 18.00 МСК, в пятницу с 9.00 до 16.45 МСК, в Рабочие предпраздничные дни режим работы сокращен на 1 час;
- в службу круглосуточной клиентской поддержки процессингового центра по телефону +7 (495) 23-23-7-23.

В данном случае деактивируется только Токен Карты Банка, 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 / Face ID/ иных биометрических систем аутентификации или другого безопасного метода блокировки/разблокировки Мобильного устройства;
- установить надежный 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;
- если для разблокировки Мобильного устройства используются биометрические данные, убедиться, что на Мобильном устройстве зарегистрированы только его 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 с Мобильного устройства, использование которого прекращено;
- осуществить Блокировку Карты / деактивацию Токена 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 / права на выполнение всех без исключения операций во всех файлах операционной системы (доступ уровня root) или реализована операция, дающая доступ к файловой системе для целей расширения возможностей устройства (джейлбрейк).

6.2 Безопасность информации, предоставленной или хранимой провайдерами, или другими третьими лицами в связи с использованием СМП находится вне контроля Банка.

7. ПРАВА И ОБЯЗАННОСТИ СТОРОН

7.1 **Банк обязан:**

7.1.1 Исполнять распоряжения Клиента по операциям в СМП, совершенным с использованием Токена.

7.1.2 Принять все возможные меры к недопущению приема распоряжений с использованием Токена 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 в соответствии с п. 5.2 об утрате Мобильного устройства, компрометации Пароля и (или) утраты контроля над SIM-картой заблокировать Токены Карт Банка на данном Мобильном устройстве.

7.1.4 Осуществлять консультирование Клиента по вопросам регистрации Карт в СМП.

7.1.5 В целях исполнения требований законодательства Российской Федерации информировать Клиентов о совершении каждой операции с использованием Токена Карты в СМП следующими способами:

- уведомление посредством отправки SMS–сообщений на Номер мобильного телефона и/или
- уведомление путем размещения информации в личном кабинете Клиента в Системе ДБО «МФК-Онлайн» и/или
- уведомление посредством отражения информации в Выписке из СКС, сформированной на бумажном носителе при обращении Клиента в Банк.

7.1.6 Обеспечить конфиденциальность информации об операциях, совершенных с использованием Токена 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 Токена Карты в СМП в случае:

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

7.2.2 В одностороннем порядке изменять настоящие Условия, уведомив Клиента о таких изменениях не менее чем за 5 (Пять) календарных дней до даты введения их в действие путем размещения на информационных стендах Банка, а также на Официальном сайте Банка либо иным способом по усмотрению Банка. Клиент соглашается со всеми изменениями, если он продолжает использование Токена Карты в СМП. Если Клиент не согласен принять изменения настоящих Условий, он должен удалить все данные Карты из СМП.

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 любое время без уведомления и по любой причине ограничить, приостановить или прекратить использование Токена Карты в СМП, Блокировать Карту, в том числе, если Клиент нарушает настоящие Условия, Договор.
7.2.5 Отказать Клиенту в регистрации Карты / формировании Токена для совершения платежей в СМП при неуспешной Верификации Карты / Верификации Клиента.
7.2.6 В любое время изменить тип 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 данных, 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.
7.3.3 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 Рабочего дня, следующего за днем получения от Банка уведомления о совершенной операции, сообщить об этом в Банк по телефонам +7 (495) 644-35-84, +7 (495) 287-02-60, и путем подачи заявления в офисе Банка.
Отсутствие предусмотренного настоящим пунктом сообщения со стороны Клиента лишает Клиента права на получение возмещения от Банка по операциям, совершенным без согласия Клиента.

7.3.4 В случае несанкционированного списания денежных средств с использованием Токена 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 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 торгово-сервисным предприятием;
- иные документы и информацию, которые имеют отношение к спорной ситуации или которые могут быть затребованы Банком в рамках рассмотрения заявления о спорной транзакции.

7.3.5 Регулярно отслеживать изменения, вносимые в настоящие Условия, публикуемые Банком на Официальном сайте в сети Интернет.
7.3.6 Совершать операции по Карте строго в пределах Расходного лимита.
7.3.7 Не позднее следующего Рабочего дня, следующего за днем изменений, информировать Банк об изменении Номера мобильного телефона и/или прекращении обслуживания Номера мобильного телефона Клиента оператором сотовой связи, замены SIM-карты. Банк, получив указанную информацию, имеет право приостановить предоставление услуги SMS-информирования до момента подтверждения принадлежности Номера мобильного телефона Клиенту, путем обращения Клиента в офис Банка.
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 СМП.
7.4.2 Приостановить /деактивировать действие Токена / Блокировать Карту, обратившись в Банк лично или по телефону. При обращении по телефону, аутентификация Клиента осуществляется в соответствии с внутренними нормативными документами Банка в соответствии с требованиями законодательства РФ.
7.4.3 Обращаться в Банк с заявлениями, в том числе при возникновении споров, связанных с операциями, совершенными с использованием Токена Карты в СМП, а также получать информацию о результатах рассмотрения заявлений, в том числе в письменной форме.

8. ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ И ОТКАЗ ОТ ГАРАНТИИ

8.1 **Клиент несет ответственность за:**

- сохранение конфиденциальности Пароля и других средств / способов Верификации Клиента;

- использование Мобильного устройства третьими лицами;
- за операции, совершенные Клиентом в СМП с использованием Токена 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 Клиентами прямо или косвенно за любые обстоятельства, при которых прерывается или нарушается функционирование СМП, например, недоступность СМП 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 Клиента, а также не предоставляет никаких заверений или гарантий по отношению к вышеупомянутому;
- за любые понесенные убытки (если иное не предусмотрено законом) связанные с использованием или невозможностью использования СМП, вне зависимости от причин и оснований возникновения ответственности;
- за убытки, которые может понести Клиент в результате отказа торгово-сервисного предприятия в возможности совершения операций с использованием СМП.
- за конфиденциальность информации, хранящейся на Мобильном устройстве, в том числе в Приложениях Apple Wallet / Google Pay.

8.3 Провайдеры предоставляют СМП и несут полную ответственность за ее функционирование. Банк не несет ответственности при нарушении провайдерами правил безопасности влияющих на любую собранную, сохраненную или отправленную в связи с использованием СМП информацию.

9. СБОР, ИСПОЛЬЗОВАНИЕ И ПЕРЕДАЧА ИНФОРМАЦИИ

9.1 Сбор, использование и передача информации о Клиенте регулируется Политикой Банка в области обработки и обеспечения безопасности персональных данных. Кроме того, Клиент соглашается с тем, что Банк вправе собирать, использовать и передавать информацию о Клиенте, в том числе информацию, относящуюся к Карте Клиента и использованию СМП, а также обмениваться данной информацией с Клиентом, с платежной системой в следующих целях:

- для подтверждения личности Клиента;
- для оказания содействия при любой покупке или иной операции с использованием Карты в рамках СМП при выполнении своих обязательств и реализации своих прав в соответствии с соглашениями, заключенными с Клиентом и Банком.

9.2 Добавляя свою Карту в СМП, Клиент понимает и соглашается с тем, что Банк вправе собирать, использовать и передавать информацию для указанных выше целей. Для получения дополнительной информации Клиент может обратиться к Политике Банка в области обработки и обеспечения безопасности персональных данных, размещенной на Официальном сайте Банка в сети Интернет.

10. ТОВАРНЫЙ ЗНАК

10.1 Apple, Apple Pay, Apple Wallet, Touch ID и Face ID являются товарными знаками компании Apple Inc., зарегистрированными в США и других странах.

10.2 Google Pay является товарным знаком Google Inc.