

## УСЛОВИЯ СОЗДАНИЯ, ОБСЛУЖИВАНИЯ ВИРТУАЛЬНЫХ КАРТ / ТОКЕНОВ И ПРОВЕДЕНИЯ ОПЕРАЦИЙ С ИХ ИСПОЛЬЗОВАНИЕМ

### 1. Термины и определения.

1.1. **Аутентификационные данные** – пароли/ отпечаток пальца/ эталон лица/ радужка глаза/ смарт-сканирование, а также другие данные, используемые по выбору Держателя для Верификации Держателя в Системе Мобильных платежей при совершении операции, исходя из возможностей и настроек его Мобильного устройства/ Носимого девайса. Аутентификационные данные являются аналогом собственноручной подписи Держателя.

1.2. **Банк** – ББР Банк (Акционерное Общество).

1.3. **Банкомат** – в рамках настоящих условий – автоматическое устройство для осуществления бесконтактных операций, обеспечивающее возможность выдачи, приема наличных денежных средств, оплаты услуг, определенных в меню Банкомата или перевода денежных средств с использованием Мобильного устройства с активным Токеном. Операции с использованием Мобильного устройства проводятся при наличии технической возможности банкомата.

1.4. **Бесконтактная операция** – Операция, при которой между платежным терминалом и процессором карты или Мобильным телефоном с технологии NFC, производится обмен данными.

1.5. **Верификация Держателя** – процедура подтверждения полномочий (предоставление прав доступа) Держателя. При регистрации Карты Верификация Держателя может осуществляться путем ввода Держателем Одноразового кода, направленного на номер мобильного телефона Держателя, сведения о котором были предоставлены Держателем при заключении Договора по карте или в процессе обновления Банком информации о Держателе. Время действия Одноразового кода является ограниченным и определяется Банком. Применение Одноразового кода является однократным. При совершении операции Верификация Держателя осуществляется с использованием Аутентификационных данных или собственноручной подписью на чеке/ слипе.

1.6. **Верификация карты** – процедура дополнительной проверки Банком Виртуальной карты, осуществляемая с целью снижения рисков проведения мошеннической операции по Карте. Верификация Карты осуществляется с применением CVC2/CVV2/ППК2 кода или без CVC2/CVV2/ППК2 кода в случае использования привязки карты через Мобильный Банк<sup>1</sup>.

1.7. **Виртуальная карта** – электронное изображение Карты, которую Клиент зарегистрировал для использования в Системе Мобильных Платежей, обладающее всеми необходимыми реквизитами для осуществления бесконтактного платежа без предъявления Карты, встроенных покупок, перевода, получения наличных.

1.8. **Держатель Карты** - Клиент или Представитель, на имя которого, в соответствии с законодательством Российской Федерации и нормативными правовыми актами Банка России, выпущена Банковская карта.

1.9. **Договор** – договор, заключаемый между Банком и Клиентом на основании и в соответствии с настоящими Условиями выпуска и обслуживания банковских карт, на основании которого Банк открывает на имя Клиента Счет, выдает Карту и осуществляет ее обслуживание.

1.10. **Банковская карта (Карта)** – эмитируемая Банком расчетная (дебетовая) карта для совершения Держателем с ее использованием или ее реквизитов операций по Счету. Банк по своему усмотрению определяет типы Карт, для которых доступно использование Системы Мобильных Платежей.

1.11. **Клиент** – физическое лицо, заключившее с Банком Договор, на имя которого, в соответствии с законодательством Российской Федерации и нормативными документами Банка России, открыт Счет в Банке (владелец Счета).

1.12. **Код подтверждения** – цифровой код в SMS-сообщении Банка, направленный на Номер мобильного телефона Клиента с целью подтверждения согласия Клиента создать к указанной Банковской карте Токен в Мобильном устройстве Клиента. Для Держателя дополнительной Карты, код подтверждения отправляется на мобильный телефон Держателя дополнительной Карты.

1.13. **Мобильное устройство** – устройство (смартфон, планшет) с поддержкой Системы Мобильных Платежей.

1.14. **Номер мобильного телефона** – зарегистрированный в Банке номер мобильного телефона Держателя, используемый для получения одноразовых паролей в рамках технологии 3D-Secure.

1.15. **Носимый девайс** - это устройство (часы, фитнес-браслет, браслет, брелок) со встроенным чипом NFC, которое может быть зарегистрировано в Системе Мобильных платежей и которое Клиент использует для оплаты покупки Бесконтактным платежом, Получения наличных, при условии регистрации Карты в Системе Мобильных Платежей, установленной на Мобильное устройство Клиента.

<sup>1</sup> Способ верификации карты определяется Провайдером Токена.

- 1.16. **Оператор сотовой связи** - компания, предоставляющая услуги сотовой связи для сотовых телефонов/ мобильных устройств своих абонентов.
- 1.17. **Провайдер Токена** – Платежная система или компания, являющаяся производителем и/или поставщиком программного обеспечения, необходимого для совершения Бесконтактных платежей, Переводов, Получения наличных в Системе Мобильных Платежей, и с которой Банком заключен договор.
- 1.18. **Процессинговый центр Банка** - независимый Процессинговый Центр (АО «КОКК»), обслуживающий операции с Банковскими картами Банка в соответствии с соглашением между Банком и Процессинговым Центром.
- 1.19. **Пункт выдачи наличных (ПВН)** – в рамках настоящих Условий - место (касса любой кредитной организации) совершения бесконтактных операций по приему, выдаче наличных денежных средств с использованием Мобильного устройства с активным Карточным токеном. Операции с использованием Мобильного устройства проводятся при наличии технической возможности Банка.
- 1.20. **Сайт Банка** – официальный сайт ББР Банка (АО) в информационно–телекоммуникационной сети «Интернет» по адресу <https://bbr.ru>.
- 1.21. **Система Мобильных Платежей** – мобильное приложение, разработанное Провайдером Токена, и программное обеспечение, предустановленное в POS-терминале, которые позволяют осуществлять бесконтактные платежи, переводы, встроенные покупки и операции получения наличных.
- 1.20. **Токен** – специальный цифровой код, заменяющий номер Карты, который формируется по факту регистрации Карты, и который хранится в зашифрованном виде в защищенном хранилище Мобильного устройства.
- 1.21. **Торгово-сервисное предприятие (ТСП)** - организация, обеспечивающая техническую возможность поддержки технологии NFC для оплаты продаваемых товаров или услуг с применением Мобильных устройств с активными токенами. Операции с использованием Мобильного устройства проводятся при наличии технической возможности ТСП.
- 1.22. **Условия** – действующие «Условия создания, обслуживания Токенов и проведения операций с их использованием ББР Банк (АО)».
- 1.24. **NFC (near field communication — англ. «ближняя бесконтактная связь»)** — технология совершения бесконтактных операций с помощью Карты или Мобильного устройства.

## 2. Общие положения.

2.1. Настоящие Условия определяют:

- процесс регистрации Карты/ создания Виртуальной карты в Системе Мобильных Платежей, установленной на Мобильном устройстве, при котором Клиент принимает Условия полностью;
- порядок совершения и подтверждения Бесконтактного платежа, выполняемого Клиентом с использованием Виртуальной карты посредством Системы Мобильных Платежей;
- порядок подтверждения Перевода, выполняемого Клиентом с использованием Виртуальной карты посредством Системы Мобильных Платежей и Мобильного Банка;
- порядок Получения наличных с использованием Виртуальной карты посредством Системы Мобильных Платежей;
- ответственность Клиента и Банка при осуществлении бесконтактного платежа, перевода с использованием Виртуальной карты посредством Системы Мобильных Платежей;
- требования к безопасности использования Мобильного устройства при совершении платежей с использованием Виртуальной карты посредством Системы Мобильных Платежей.

2.2. Банк не является владельцем Токена, владельцем Провайдера Токена, провайдером Системы Мобильных Платежей и не осуществляет поддержку программного обеспечения Системы Мобильных Платежей, установленного на Мобильном устройстве Клиента, в котором хранится Токен. Установка и использование мобильного приложения для доступа к Системе Мобильных Платежей на Мобильном устройстве осуществляется в соответствии с правилами и в порядке, установленном Провайдером Токена.

2.3. Банк не взимает комиссию за совершение операций с использованием Виртуальной карты посредством Системы Мобильных Платежей. При Получении наличных комиссия взимается в соответствии с Тарифами.

2.4. Условия действуют до расторжения Договора по карте. Прекращение действия Условий не влияет на юридическую силу и действительность распоряжений, направленных в Банк Клиентом до прекращения действия Условий.

2.5. В случае несоответствия между любыми положениями Условий и законодательством Российской Федерации и/или правилами Платежной системы Банк имеет право изменить Условия

в одностороннем порядке с целью приведения их в соответствие с законодательством Российской Федерации и/или правилами Платежной системы.

### 3. Регистрация карт

3.1. Клиент устанавливает в Мобильном устройстве Систему Мобильных Платежей (если ранее в Мобильном Устройстве не была установлена Система Мобильных Платежей), путем скачивания из системы официального онлайн-магазина мобильных приложений.

3.2. Для осуществления бесконтактного платежа, встроенной покупки, перевода, выдачи наличных с использованием Системы Мобильных Платежей Клиенту необходимо выбрать один из способов Верификации Держателя в Системе Мобильных платежей - с использованием пароля/ отпечатка пальца/ эталона лица/ радужки глаза/ сканирования, других данных, используемых для доступа в Систему Мобильных платежей.

3.3. Клиент выполняет регистрацию Карты в Системе Мобильных Платежей одним из способов:

- путем автоматического ввода Номера Карты с использованием камеры Мобильного устройства;
- вводом Номера Карты вручную;
- иным способом, определяемым Платежной системой/ Провайдером Токена, при наличии у Банка технической возможности.

Далее Клиент указывает данные, нанесенные на Карту: фамилию и имя Держателя, срок действия Карты и CVC2/ CVV2/ППК2 код.

3.4. Для подтверждения действительности Карты осуществляется Верификация Карты с помощью Технологии CVC2/ CVV2/ППК2 кода. Карта должна быть активна, иметь не истекший срок действия.

3.5. После выполнения Клиентом действий, указанных в пунктах 3.2-3.3 Условий, осуществляется Верификация Держателя и активация Токена путем ввода Клиентом Одноразового кода, отправленного Банком в SMS-сообщении на номер мобильного телефона, предоставленный Держателем при заключении с Банком Договора по Карте или в процессе обновления Банком информации о Держателе.

Подробная информация о регистрации Карты Клиента доступна в сети интернет на официальных страницах Платежных систем и/или Провайдера Токена.

3.6. По факту успешной регистрации Карты формируется Виртуальная карта и Токен, который хранится в защищенном хранилище Мобильного устройства или защищенном облачном хранилище Провайдера Токена. Токен позволяет однозначно идентифицировать Карту, используемую при совершении Бесконтактных платежей, Встроенных покупок, Перевода, Получения наличных с помощью Системы Мобильных Платежей. О факте успешной регистрации Карты Банк направляет Держателю SMS-сообщение на номер Мобильного устройства.

3.7. Регистрация Карты в Носимом девайсе<sup>2</sup> осуществляется Клиентом одним из способов, предлагаемых производителем Носимого девайса:

- в мобильном приложении Провайдера Токена после регистрации Карты в Системе Мобильных платежей в порядке, установленном п.п. 3.3-3.4 настоящих Условий после выполнения активации Носимого девайса в мобильном приложении Провайдера Токена, установленном на Мобильном устройстве.

После получения в Системе Мобильных платежей сообщения об успешной регистрации и активации Карты для используемого Носимого девайса Виртуальная Карта может использоваться в Носимом девайсе. Провайдер Токена может ограничить количество Карт, используемых в одном Носимом девайсе.

3.8. На одно Мобильное устройство с установленной Системой Мобильных Платежей можно зарегистрировать несколько<sup>3</sup> Карт, эмитированных Банком.

3.9. Одну и ту же Карту можно регистрировать в нескольких Системах Мобильных Платежей, доступных Клиенту.

3.10. Клиент может самостоятельно удалить из Системы Мобильных Платежей одну или несколько Виртуальных карт.

Изображение Виртуальной карты в Системе Мобильных Платежей может не соответствовать реальному дизайну Карты, и содержит маскированный Номер Карты (отображены 4 последние цифры Номера карты).

<sup>2</sup> Не все Носимые девайсы поддерживают все варианты регистрации Карты (за дополнительной информацией необходимо обращаться к производителю Носимого девайса). Процесс активации Носимого девайса для технической привязки Токена к Носимому девайсу зависит от используемого Клиентом Носимого девайса

<sup>3</sup> Количество Карт для регистрации в Системе Мобильных Платежей может изменяться по решению Провайдера Токена либо по решению Банка.

#### **4. Совершение операций с использованием Виртуальной карты посредством Системы Мобильных Платежей**

4.1. Бесконтактные платежи с использованием Виртуальной карты в Системе Мобильных Платежей могут осуществляться через POS-терминал, оснащенный технологией NFC («ближняя бесконтактная связь»).

4.2. Для осуществления Бесконтактных платежей с помощью Виртуальной карты Клиент открывает на Мобильном устройстве/ Носимом девайсе (если это предусмотрено технологией устройства) Систему Мобильных Платежей. Выбирает для оплаты покупок необходимое изображение Виртуальной карты (если это предусмотрено технологией устройства) и, разместив Мобильное устройство/ Носимый девайс рядом с POS-терминалом, подтверждает совершение операции вводом Аутентификационных данных.

Для осуществления Встроенных покупок Клиент выбирает Виртуальную карту в Системе Мобильных Платежей и подтверждает оплату путем ввода Аутентификационных данных.

Для осуществления Перевода Клиент осуществляет действия, описанные в Условиях по переводам в Мобильном Банке, подтверждает свое желание осуществить перевод путем ввода Аутентификационных данных.

4.3. Для Получения наличных в Банкомате, оснащенный технологией NFC, Клиент открывает на Мобильном устройстве/ Носимом девайсе (если это предусмотрено технологией устройства) Систему Мобильных платежей, при необходимости выбирает изображение Виртуальной карты, вводит в Мобильном устройстве/ Носимом девайсе Аутентификационные данные в целях проведения Верификации Держателя, прикладывает Мобильное устройство/ Носимый девайс к метке NFC на Банкомате, вводит в Банкомате ПИН-код Карты.

Выбирает операцию Получение наличных, вводит необходимую сумму и получает наличные денежные средства, следуя подсказкам меню Банкомата.

4.4. Операции, совершенные с использованием Виртуальной карты и Аутентификационных данных, считаются операциями Клиента.

4.5. Система Мобильных Платежей предоставляет Клиенту доступ к данным о совершенных Бесконтактных платежах, Переводах, Встроенных покупках, операциях Получения наличных, а также предоставляет следующую информацию:

4.5.1. о статусе Карты/ Виртуальной карты;

4.5.2. о возможности подключения/ отключения уведомления об операциях по каждой Виртуальной карте.

Система Мобильных Платежей не предоставляет информацию об операциях, совершенных не с помощью Системы Мобильных Платежей.

4.6. Иные условия проведения операций с использованием Карты, не урегулированные в настоящем разделе Условий, изложены в заключенном с Клиентом Договоре по карте.

4.7. Банк не взимает плату за использование Виртуальной карты, Условиях по переводам.

#### **5. Блокировка Токена / Мобильного устройства / Носимого девайса**

5.1. В случае утраты Карты/ компрометации Карты<sup>4</sup>/ использования Карты без согласия Клиента Клиент обязуется незамедлительно осуществить действия, предусмотренные соответствующим Договором по карте.

С момента блокировки Карты блокируются все Токены/ Виртуальные карты для данной Карты на всех Мобильных устройствах/ Носимых девайсах с целью недопущения совершения операций.

5.2. В случае утраты Мобильного устройства или утраты управления Мобильным устройством, Клиенту необходимо обратиться в Банк в порядке, указанном выше, с целью блокировки Виртуальной карты.

5.3. В случае утраты Носимого девайса необходимо заблокировать Носимый девайс через Систему Мобильных платежей, установленную на Мобильном устройстве. При блокировании Носимого девайса Карта не блокируется.

#### **6. Требования к безопасности**

6.1. Организационные меры по защите информации, реализуемые Клиентом:

- не оставлять Мобильное устройство/ Носимый девайс без присмотра в разблокированном виде;
- обеспечить соответствующий уровень безопасности на Мобильном устройстве/ Носимом девайсе, используя Пароли и другие возможные методы блокировки/ разблокировки;

<sup>4</sup> Незаконное получение третьими лицами информации о реквизитах Карты.

- убедиться, что на Мобильном устройстве/ Носимом девайсе не зарегистрированы Отпечатки пальцев/ Эталоны лица/ Радужки глаз или иные способы разблокировки Мобильного устройства/ Носимого девайса другого лица;
- не разглашать третьим лицам регистрационные данные от Мобильного устройства/Носимого девайса, если прекращено их использование (это конфиденциальная информация);
- удалить все личные данные и финансовую информацию со старого Мобильного устройства/Носимого девайса, если прекращено их использование;
- незамедлительно обратиться в Банк по номеру телефона, указанному на оборотной стороне Карты, либо по номеру телефона Банка, указанному на сайте Банка, в случае подозрений на любое несанкционированное использование Мобильного устройства/ Носимого девайса, а также, если Мобильное устройство/ Носимый девайс были взломаны, потеряны или украдены (необходимо заблокировать Карты, удалить Токен, чтобы избежать несанкционированного использования Виртуальной карты);
- не блокировать любые функции безопасности, предусмотренные приложениями Мобильных устройств/ Носимых девайсов, для использования этих функций и процедур безопасности для защиты всех Виртуальных карт;
- создать Пароль, соответствующий требованиям Провайдера Токена;
- удалять информацию обо всех Виртуальных картах при передаче Мобильного устройства/ Носимого девайса третьим лицам;
- не устанавливать на Мобильное устройство программы повышения прав пользователя, не заложенные производителем Мобильного устройства (привилегий взлома операционной системы устройства (rooting));
- в случае утери Мобильного устройства Клиент может заблокировать приложение Провайдера Токена и/или удалить все данные из Системы Мобильных Платежей с помощью функции удаленного поиска Мобильного устройства с целью предотвращения использования Виртуальной карты посредством Системы Мобильных Платежей третьими лицами;
- в случае утери Носимого девайса Клиент может заблокировать Носимый девайс через приложение Провайдера Токена;
- не сообщать реквизиты Карты третьим лицам и не регистрировать Карту на Мобильных устройствах/ Носимых девайсах, принадлежащих третьим лицам;
- никому (в т.ч. сотрудникам Банка) не сообщать Одноразовый код, полученный при регистрации Карты в Системе Мобильных Платежей.

## **7. Права и обязанности сторон**

### **7.1. Банк обязан:**

7.1.1. Исполнять распоряжения Клиента по операциям, совершаемым с использованием Виртуальной карты посредством Системы Мобильных Платежей в соответствии с Договором по карте, Условиями по переводам.

7.1.2. Принять все возможные меры к недопущению приема распоряжений с использованием Виртуальной карты посредством Системы Мобильных Платежей без предварительной успешной Верификации Клиента.

7.1.3. Незамедлительно, но не позднее 30 (тридцати) минут с момента получения обращения Клиента об утрате Мобильного устройства, компрометации Карты/ Пароля и (или) утраты контроля над SIM-картой заблокировать Токены/ Виртуальные карты на данном Мобильном устройстве. При обращении Клиента по телефону установление личности Клиента и подтверждение его полномочий осуществляется в соответствии с внутренними регламентными документами Банка.

7.1.4. Осуществлять консультирование Клиента по вопросам регистрации Карт в Системе Мобильных Платежей, активации Токена и по использованию Носимых девайсов.

7.1.5. Обеспечить конфиденциальность информации об операциях, совершенных с использованием Виртуальной Карты посредством Системы Мобильных Платежей.

7.1.6. Предоставлять по письменному требованию Клиента документы, связанные с совершением операций с использованием Виртуальной карты посредством Системы Мобильных Платежей в срок не позднее 30 дней со дня получения Банком соответствующего запроса.

### **7.2. Банк имеет право:**

7.2.1. Не исполнять распоряжения Клиента, совершенные с использованием Виртуальной карты в Системе Мобильных Платежей в случае:

- если Верификация Держателя/ Верификация Карты не осуществлена;

- если Клиентом не соблюдены требования законодательства Российской Федерации в случае проведения платежей, не соответствующих режиму Счета, приобретению товаров/ работ/ услуг, запрещенных законодательством Российской Федерации;

- если не соблюдены требования настоящих Условий, положений Договора по карте.

7.2.2. В целях обеспечения безопасности устанавливать:

- ограничения по времени действия Одноразового кода в пределах одного сеанса соединения (тайм-аут);

- лимиты/ ограничения на проведение операций с использованием Виртуальной карты в соответствии с Тарифами.

7.2.3. В установленных законодательством Российской Федерации случаях осуществлять в отношении Клиента контрольные и иные функции, возложенные на Банк законодательством Российской Федерации, в связи с чем запрашивать у Клиента любые необходимые документы и (или) письменные пояснения относительно характера и экономического смысла предполагаемых или совершенных операций с использованием Виртуальной Карты посредством Системы Мобильных Платежей.

7.2.4. В любой момент потребовать от Клиента подписания документов на бумажном носителе, эквивалентных по смыслу и содержанию электронным распоряжениям, подписанным ЭП Клиента, переданными Клиентом через Систему Мобильных Платежей и исполненными Банком.

7.2.5. Заблокировать, ограничить, приостановить или прекратить использование Виртуальной Карты/ Карты, если Клиент нарушает настоящие Условия, в случае наличия подозрений на несанкционированное использование Виртуальной карты и/или Карты.

7.2.6. Отказать Клиенту в регистрации Карты для совершения операций в Системе Мобильных Платежей, в том числе при неуспешной Верификации Держателя/ Верификации Карты.

7.2.7. В случае неисполнения Клиентом п.7.3.7. настоящих Условий, Банк имеет право приостановить совершение операций по Виртуальной Карте в Системе Мобильных Платежей.

### **7.3. Клиент обязан:**

7.3.1. Соблюдать положения Условий;

7.3.2. До регистрации Карты в Системе Мобильных платежей Клиент обязан убедиться, что в качестве Аутентификационных данных используются Отпечаток пальца/ Эталон лица/ Радужка глаза/ Смарт-сканирование именно Клиента.

7.3.3. Обеспечить конфиденциальность, а также хранение Мобильного устройства/ Носимого девайса, Аутентификационных данных, SIM-карты способом, исключающим доступ к ним третьих лиц, а также немедленно уведомлять Банк о подозрении, что Мобильное устройство, Карта, Пароль, ПИН-код, SIM-карта могут быть использованы посторонними лицами.

В случае утраты Клиентом Мобильного устройства или наличия подозрений, что они используются третьими лицами, Клиент должен незамедлительно после обнаружения указанных фактов сообщить об этом Банку, используя один из способов обращения, предусмотренных в п.5.1. Условий.

На основании указанного выше сообщения Клиента Банк в срок, указанный в п. 7.1.3 Условий, блокирует Токен/ Виртуальную карту. В случае утери Носимого девайса Клиент самостоятельно блокирует Носимый девайс через Систему Мобильных платежей.

7.3.4. В случае несанкционированного списания денежных средств с использованием Виртуальной Карты посредством Системы Мобильных Платежей 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/ 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 из торговой организации;

- иные документы и информацию, которые имеют отношение к спорной ситуации или которые могут быть разумно затребованы Банком в рамках рассмотрения заявлений о несанкционированных списаниях.

7.3.5. Регулярно, но не реже 1 (одного) раза в месяц, обращаться в Банк за получением информации об имевших место изменениях и дополнениях в Условиях.

7.3.6. Контролировать соответствие суммы операции и текущего остатка на Счете и осуществлять операции в Системе Мобильных Платежей только в пределах этого остатка. При отправке поручений контролировать достаточность средств на Счет для одновременного списания суммы операции и суммы комиссии за данную операцию в соответствии с Тарифами.

7.3.7. Сообщать Банку об изменении номера мобильного телефона Клиента, прекращении обслуживания номера мобильного телефона Клиента оператором мобильной связи или замены SIM-карты<sup>5</sup>(IMSI) в течение 3 (трех) рабочих дней со дня совершения соответствующих изменений. Банк, получив указанную информацию, имеет право приостановить использование Виртуальной карты посредством Системы Мобильных Платежей до момента подтверждения Клиентом принадлежности номера мобильного телефона способами, предусмотренными Договором по карте.

7.3.8. Незамедлительно предоставлять по требованию Банка документы и (или) письменные пояснения относительно характера и экономического смысла предполагаемых или совершенных операций в Системе Мобильных Платежей.

7.3.9. Представлять информацию, а также документы (сведения), необходимые для исполнения Банком требований Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», требований нормативно-правовых актов Банка России, включая информацию о своих выгодоприобретателях, бенефициарных владельцах, представителей Клиента.

7.3.10. Исполнять требования, изложенные в разделе 6 настоящих Условий.

#### **7.4. Клиент имеет право:**

7.4.1. Обращаться в Банк для получения дополнительной информации/ консультаций по работе в Системе Мобильных Платежей, обратившись в Банк по телефонам, указанным на официальном интернет-сайте Банка <https://bbr.ru>.

7.4.2. Приостановить действие Токена/ Виртуальной карты, обратившись в Банк лично или по телефону, указанному на официальном интернет-сайте Банка. При обращении по телефону идентификация и аутентификация Клиента осуществляется аналогично порядку, предусмотренному п.9.3. Правил КБО.

---

<sup>5</sup> Подтвердить смену SIM-карты (IMSI - International mobile subscriber identity) номера мобильного телефона, Держатель может способами, указанными в Договоре по карте.