

*Правила действуют
с «21» марта 2016г.*

**ПРАВИЛА
использования Карты клиента,
работы в Сервисе «Интернет Платежи»
и в Сервисе «Мобильные платежи»**

Настоящие Правила использования Карты клиента, работы в Сервисе «Интернет Платежи» и в Сервисе «Мобильные платежи» (далее – Правила), являются неотъемлемой частью Договора о комплексном обслуживании клиента (далее – Договора).

Термины и определения

PUSH-сообщение – короткое текстовое сообщение, передаваемое на Устройство с использованием технологий Apple Push Notification Service (для операционной системы iOS) и Google Cloud Messaging (для операционной системы Android OS).

Идентификация – процедура получения Клиентом доступа к Сервису «Интернет Платежи», осуществляемая с использованием Логина и Пароля. Факт успешного прохождения Идентификации подтверждает, что операции в рамках Сервиса «Интернет Платежи» осуществляются Клиентом лично.

Мобильное приложение – разработанное правообладателем ЗАО «Биллинговый центр» (Место нахождения: 630128, г. Новосибирск, ул. Инженерная, д. 4а) программное обеспечение, предназначенное для получения Клиентом доступа к Платежному кабинету с помощью Устройства. Клиент может установить Мобильное приложение самостоятельно, только в Google Play и AppStore (официальное приложение «Кукуруза» или «Карта Билайн» в зависимости от Карты клиента). В Google Play и AppStore приложение «Кукуруза» распространяет ООО «Евросеть-Ритейл» (Место нахождения: 125284, г. Москва, ул. Береговая, д.3, стр. 1, 36 этаж), а приложение «Карта Билайн» - ПАО «ВымпелКом» (Место нахождения: 127083, г. Москва, ул. Восьмого Марта, дом 10, строение 14), на основании соответствующего договора с правообладателем (ЗАО «Биллинговый Центр»).

Код активации – размещенный на Карте клиента код, который используется для присоединения Клиента к Договору, если это предусмотрено его условиями.

Компрометация ключевой информации: Пароля, Разового секретного пароля, PIN-кода – утрата РНКО или Клиентом уверенности в том, что Пароль и/или Разовый секретный пароль и/или PIN-код не может быть использован третьими лицами.

Логин – тринадцатизначный номер (EAN), нанесенный на обратной стороне Карты клиента. Для Мобильного приложения в качестве Логина используется совокупность EAN и Уникального идентификатора Мобильного приложения. Клиент вправе использовать в качестве Логина Номер мобильного телефона, если это предусмотрено Правилами Сервиса «Интернет Платежи». Допускается наличие у Клиента более одного Логина. В таком случае, действие, совершенное Клиентом под любым из Логин, имеет равную силу и влечет одинаковые юридические последствия.

Номер мобильного телефона – номер мобильного телефона Клиента, указанный Клиентом при заключении Договора либо измененный в порядке, установленном Договором.

Отчет – отчет РНКО по операциям, учтенным в Электронном кошельке, за определенный период времени.

Пароль – секретная последовательность символов, которая известна только Клиенту. Для каждого Логина устанавливается Пароль, который позволяет убедиться в том, что обратившееся лицо действительно является владельцем представленного Логина.

Платежный кабинет – часть программно-аппаратного комплекса Системы, предназначенная для управления Клиентом в рамках Сервиса «Интернет Платежи» своим Электронным кошельком, доступная после Идентификации Клиента. Доступ к Платежному кабинету возможен с использованием следующих каналов: Интернет-сайт, указанный в Договоре, и/или Мобильное приложение.

Разовый секретный пароль – уникальный набор символов, предоставляемый Клиенту РНКО для подтверждения направления Клиентом РНКО Распоряжения о переводе ЭДС, Распоряжения о возврате остатка ЭДС, подтверждения иного волеизъявления в предусмотренных Договором случаях, с использованием Карты клиента (или Реквизитов Карты клиента) или Сервиса «Интернет Платежи». Разовый секретный пароль имеет ограниченный срок действия.

Система - программно-аппаратный комплекс РНКО, позволяющий организовать обмен документами в электронной форме (в том числе ЭПД) между РНКО и Клиентом в рамках Сервиса «Интернет Платежи».

Уникальный идентификатор Мобильного приложения – уникальная для каждой инсталляции Мобильного приложения последовательность латинских букв и цифр, которая формируется автоматически в момент установки Мобильного приложения на устройство Клиента.

Устройство – мобильный персональный компьютер Клиента, дополненный функциональностью мобильного телефона (смартфон, коммуникатор, планшетный компьютер и т.п.), работающий под управлением операционной системы iOS (версии не ниже iOS7), или Android OS, или watchOS. Устройство с операционной системой watchOS (наручные часы с дополнительной функциональностью (умные часы)) далее будет именоваться AppleWatch.

Электронный платежный документ (ЭПД) – электронное сообщение, сформированное Клиентом в Платежном кабинете и содержащее одно или несколько Распоряжений о переводе ЭДС или Распоряжений о возврате остатка ЭДС. Неизменность, правильность, целостность и авторство ЭПД удостоверяется вводом Пароля при Идентификации и/или Разового секретного пароля.

Клиент соглашается с тем, что Пароль и Разовый секретный пароль являются аналогом собственноручной подписи.

Термины, не определенные в настоящих Правилах, применяются в том значении, в котором они определены в Договоре. Во всех иных случаях такие термины применяются в том значении, в каком они используются в соответствующей отрасли законодательства Российской Федерации.

1. Общие меры безопасности и защиты от мошенничества

1.1. Рекомендуется хранить Карту клиента в недоступном для окружающих месте, не передавать Карту клиента другому лицу, за исключением продавца (кассира).

Рекомендуется хранить Карту клиента отдельно от наличных денег и документов, а также от PIN-кода, Кодового слова.

Во избежание мошенничества с использованием Карты клиента Клиенту рекомендуется проводить операции с ней только в своем присутствии, не позволять уносить Карту клиента из поля зрения.

1.2. Во избежание использования Карты клиента другим лицом необходимо хранить и использовать PIN-код способами, обеспечивающими невозможность его несанкционированного использования, в том числе – не передавать в пользование третьим лицам Карту клиента, не сообщать PIN-код другим лицам, не вводить PIN-код при работе в сети Интернет.

1.3. При проведении операции с вводом PIN-кода рекомендуется прикрывать клавиатуру свободной рукой.

1.4. При подозрении на возможное использование Карты клиента (или Реквизитов Карты клиента) посторонними лицами необходимо незамедлительно заблокировать Электронное средство платежа в порядке, предусмотренном Договором.

1.5. Перед началом проведения операции в устройстве самообслуживания рекомендуется осмотреть его лицевую часть, в частности, поверхность над клавиатурой и устройство для приема карты в устройстве самообслуживания. В названных местах не должно находиться прикрепленных посторонних предметов. В случае обнаружения подозрительных прикрепленных посторонних предметов Клиенту не рекомендуется проводить операцию.

1.6. Предъявлять Карту клиента, сообщать номер и другие Реквизиты Карты клиента необходимо только в момент проведения операции, которую Клиент считает надежной и правомерной. Клиент не должен сообщать Реквизиты Карты клиента, Разовый секретный пароль, Кодовое слово, свои персональные данные, если ему позвонили и назвали представителем какой-либо организации, включая РНКО или Агента.

Если Клиент получил через сеть Интернет электронное сообщение с предложением предоставить персональные данные и EAN Карты клиента для того, чтобы зарегистрироваться для предоставления услуг или обновления персональных данных, необходимо выяснить правомерность таких предложений, позвонив в Информационный Центр. Реквизиты Карты клиента в таких случаях Клиент сообщать не должен, т.к. они запрашиваются только для совершения операций.

1.7. Рекомендуется не использовать для совершения операций чужие компьютеры. Особенно это касается интернет-кафе и компьютеров общего доступа.

1.8. Необходимо установить на компьютер и Устройство антивирусные программы и своевременно их обновлять. Также рекомендуется регулярно обновлять операционную систему. Делается это во избежание заражения компьютера вирусами, что может повлечь разглашение третьим лицам Реквизитов Карты клиента, Логина, Пароля.

1.9. При введении данных Карты клиента, Логина и Пароля необходимо обращать внимание на адресную строку браузера. Конфиденциальная финансовая информация должна передаваться по защищенному соединению. В этом случае вы увидите специальный значок «замка», а адрес сайта в обязательном порядке будет начинаться с префикса <https://>.

1.10. По возможности, необходимо запоминать или проверять часто используемые адреса интернет-магазинов и своего интернет-банка (Платежного кабинета). Поскольку мошенники могут заменить в адресе всего 1-2 символа, а вы попадете на совершенно другой (мошеннический) сайт, в т.ч. сайт-двойник.

1.11. В целях обеспечения безопасного проведения операций с использованием Реквизитов Карты клиента в сети Интернет Клиенту рекомендуется пользоваться сайтами торгово-сервисных предприятий, использующих технологию безопасного проведения операций по картам в сети Интернет: Verified by Visa и MasterCard SecureCode.

1.12. Перед проведением операции Клиенту самостоятельно необходимо удостовериться в надежности сайта, предлагающего возможность оплаты с использованием банковских карт, а также в том, что совершаемая операция является именно оплатой товаров и услуг. Рекомендуется использовать официальные сайты компаний.

1.13. В целях безопасности рекомендуется устанавливать собственные лимиты на совершение операций с использованием Карты клиента, если это предусмотрено Договором.

1.14. При поступлении уведомлений об операциях, совершенных без согласия Клиента, Клиенту необходимо незамедлительно направить уведомление для блокировки Электронного средства платежа в порядке, предусмотренном Договором.

1.15. Необходимо предпринимать меры по сохранности Устройства с установленным Мобильным приложением и не допускать возможности использования Мобильного приложения/Устройства третьими лицами.

1.16. Клиенту не рекомендуется устанавливать на свой компьютер, Устройство, программное обеспечение из неофициальных источников. Рекомендуется использовать лицензионное программное обеспечение.

1.17. Мобильное приложение в рамках настоящих Правил может быть установлено только в Google Play и AppStore от указанных в настоящих Правилах распространителей. В случае получения Клиентом предложения об установке любого программного обеспечения, якобы являющегося Мобильным приложением или связанного с ним, из иных источников или от других распространителей, – Клиенту необходимо незамедлительно прекратить работу с таким источником и сообщить о произошедшем в Информационный центр.

1.18. На Устройство необходимо установить надежный пароль.

2. Ответственность РНКО и Клиента

2.1. РНКО не несет ответственность за:

- неисполнение распоряжения Клиента в случаях, когда такое право предусмотрено Договором, Правилами и законодательством РФ;
- повторную ошибочную передачу Клиентом распоряжения (т.е. в случае передачи второго распоряжения в первые несколько минут после передачи первого распоряжения на ту же сумму и в пользу того же Получателя);
- предоставление Клиентом недостоверной информации, потери актуальности информации, ранее предоставленной Клиентом, используемой при регистрации и исполнении РНКО ЭПД, или вводом Клиентом неверных данных;
- ущерб, возникший вследствие несанкционированного использования третьими лицами Разового секретного пароля Клиента, если такое использование произошло после передачи Разового секретного пароля Клиенту;
- полное или частичное неисполнение, ненадлежащее исполнение своих обязательств согласно Правилам, если такое неисполнение вызвано обстоятельствами непреодолимой силы, решениями органов законодательной, судебной и/или исполнительной власти Российской Федерации, а также Банка России, которые делают невозможным для РНКО выполнение своих обязательств; задержками в зачислении денежных средств по вине иных кредитных организаций; военными действиями, стихийными или иными бедствиями, происходящими в районах, официально признанными находящимися под влиянием вышеуказанных обстоятельств;

- качество и скорость передачи информации через каналы операторов связи;
- убытки, понесенные Клиентом в связи с использованием Карты клиента и Сервисов (в том числе убытки, понесенные в результате неправомерных действий третьих лиц), за исключением случаев, когда такие убытки были причинены Клиенту в результате неисполнения/неадекватного исполнения РНКО своих обязательств;
- неисполнение продавцом товаров (услуг) своих обязательств перед Клиентом, в адрес которых РНКО исполнил распоряжения Клиента о возврате Остатка ЭДС, о переводе ЭДС;
- ущерб, связанный с установкой на Устройство Клиента какого-либо программного обеспечения, за исключением Мобильного приложения.

2.2. Ответственность Клиента

2.2.1. Клиент несет ответственность перед РНКО в соответствии с требованиями действующего законодательства Российской Федерации, в том числе за убытки, возникшие у РНКО в результате исполнения распоряжений, переданных в РНКО от имени Клиента неуполномоченным лицом с использованием принадлежащих Клиенту Логина, Пароля, Разового секретного пароля.

2.2.2. Клиент несет ответственность за правильность и актуальность всех сведений, сообщаемых им РНКО, при заключении и исполнении Договора.

2.2.3. Клиент, заключая Договор, подтверждает, что доступ к Устройство с установленным Мобильным приложением, AppleWatch с установленным приложением, имеет только Клиент; Устройство с установленным Мобильным приложением/Мобильное приложение, AppleWatch не используются третьими лицами, а также обязуется обеспечивать указанный режим пользования в течение срока действия Договора.

В случае невыполнения указанной обязанности Клиент принимает на себя риск убытков и иных неблагоприятных последствий в результате несанкционированного доступа третьих лиц к номеру мобильного телефона, SIM-карте, иному Устройство, на котором установлено Мобильное приложение, Мобильному приложению.

2.2.4. Клиент соглашается на передачу распоряжений и/или информации через сеть Интернет, в том числе с использованием Мобильного приложения, осознавая, что такие каналы не всегда являются безопасными, и соглашается нести все риски, в том числе – связанные с возможным нарушением конфиденциальности, возникающие вследствие использования таких каналов передачи информации.

ПРАВИЛА использования Карты клиента

3. Общие положения

3.1. Карта клиента может быть использована для совершения операций по правилам одной из международных платежных систем MasterCard Worldwide, VISA International или российских платежных систем «Золотая Корона», «ОБЪЕДИНЕННАЯ РАСЧЕТНАЯ СИСТЕМА», «МастерКард», Виза.

3.2. Карта клиента предназначена для проведения операций в торговых и сервисных точках, в банковских учреждениях и устройствах самообслуживания (банкоматы, информационно-платежные терминалы), на которых размещены эмблемы соответствующих платежных систем.

3.3. Срок действия Карты клиента указан на лицевой стороне карты. По истечении срока действия Карта клиента не действительна. Рекомендуется своевременно обращаться в ТОА для сдачи карты с истекшим сроком действия и получения карты, выпущенной на новый срок действия.

4. Персональный идентификационный номер (PIN-код) Карты клиента

4.1. Под компрометацией PIN-кода понимается утрата РНКО или Клиентом уверенности в том, что PIN-код не может быть использован третьими лицами.

4.2. В случае возникновения подозрений о том, что Реквизиты Карты клиента или PIN-код могли быть доступны другим лицам или скопированы, необходимо незамедлительно направить уведомление для блокировки Электронного средства платежа в порядке, предусмотренном Договором.

4.3. PIN-код не может быть затребован ни РНКО, ни любой другой организацией, в том числе при оплате товаров/услуг через Интернет и иные информационные сети (за исключением операций, проводимых в устройствах самообслуживания или электронных терминалах торгово-сервисных предприятий).

4.4. Клиент может получить новый PIN-код в случае утраты/компрометации ранее действовавшего, обратившись для этого в Информационный центр с использованием Кодового слова.

5. Активация Карты клиента

5.1. Активация Карты клиента не предусмотрена, если присоединение Клиента к Договору не предусматривает процедуру направления Кода активации, размещенного на Карте клиента.

5.2. Перед поездкой за границу или в другой город рекомендуется убедиться в том, что Карта клиента активна (не заблокирована, Срок действия Карты клиента не истек, произведено подтверждение получения/замены Карты клиента) и в рабочем состоянии. Для этого необходимо заранее провести операцию с вводом PIN -кода через устройство самообслуживания или электронный терминал.

5.3. Если в результате повреждения Карту клиента стало невозможно использовать для совершения операций, Клиенту необходимо обратиться в ТОА, для ее замены, если это предусмотрено Договором.

6. Правила работы с устройствами самообслуживания

6.1. Снятие наличных денежных средств:

Инструкции по проведению операции через банкомат (в т.ч. информация о валюте операции) последовательно появляются на экране банкомата.

После трех последовательных попыток ввода неправильного PIN-кода Карта клиента блокируется.

По завершении операции необходимо получить деньги, Карту клиента и чек устройства самообслуживания (они могут возвращаться в любом порядке). В противном случае предъявленные деньги и Карта клиента по истечении 20-40 секунд будут задержаны устройством самообслуживания.

6.2. Внесение наличных денежных средств:

При проведении операции внесения наличных через устройство самообслуживания необходимо пересчитать сумму вносимых денежных средств, расправить банкноты, не допуская загнутых краев.

На экране устройства самообслуживания указывается информация о максимальном количестве банкнот, вставляемых в модуль приема наличных единовременно.

Не допускается использовать мятые, порванные и ветхие банкноты. Не допускается вставлять в модуль приема наличных монеты и другие посторонние предметы.

По завершении операции рекомендуется получить чек (в некоторых случаях может быть два чека) и Карту клиента, проверить информацию, содержащуюся в чеке.

6.3. Если Карта клиента задержана устройством самообслуживания, Клиенту необходимо заблокировать Карту клиента. Для замены карты, если это предусмотрено Договором, необходимо обратиться в ТОА. Возврат денежных средств осуществляется в порядке, предусмотренном Договором. Рекомендуется сохранять все чеки устройств самообслуживания в течение не менее 6 месяцев (в т.ч. и чек об изъятии карты) с даты совершения операции.

7. Оплата товаров и услуг с использованием Карты клиента

7.1. В случае, если операция проводится с использованием электронного терминала, кассир может предложить Клиенту ввести PIN-код на выносной клавиатуре электронного терминала. При отказе ввести PIN-код или неверном вводе PIN-кода в операции может быть отказано. Несогласие подписать чек электронного терминала также может привести к отказу в проведении операции.

Клиент обязан ознакомиться с содержанием чека и имеет право отказаться от подписания чека, в котором не проставлены (или не соответствуют действительности) сумма, валюта, дата операции, тип операции, название торгово-сервисной точки. Дополнительно в чеке может содержаться сумма проводимой операции в валюте, отличной от местной, с указанием курса пересчета, который будет использоваться при списании Остатка ЭДС.

По завершении операции кассир должен выдать Клиенту чек.

7.2. При возврате покупки или отказе от услуг, ранее оплаченных в торгово-сервисной точке с использованием Карты клиента, должна быть проведена кредитовая операция – операция «возврат покупки» с обязательным оформлением чека (на котором указано «возврат покупки»), подписанного кассиром торгово-сервисной точки. Необходимо сохранить указанный чек. Если сумма операции не поступит в Электронный кошелек в течение 30 (Тридцати) дней, Клиент оформляет заявление через Информационный центр.

8. Оплата товаров и услуг, перевод денежных средств в сети Интернет с использованием Реквизитов Карты клиента.

8.1. Для осуществления операции клиенту необходимо ввести Реквизиты Карты клиента в соответствующие формы сайта. Если имя и фамилия держателя не нанесены на Карте клиента, то поле с фамилией и именем необходимо оставить пустым. Если фамилия и имя запрашиваются принудительно, необходимо ввести «Unembossed Name» или фамилию и имя латинскими буквами. Ввод Реквизитов Карты клиента означает, что операция совершается Клиентом лично.

8.2. Для подтверждения совершения операции может требоваться ввод Разового секретного пароля. Разовый секретный пароль при оплате с использованием Реквизитов Карты клиента направляется Клиенту в виде SMS-сообщения на Номер мобильного телефона после запроса Клиента на предоставление Разового секретного пароля (технология MasterCard Secure Code или Verified by Visa). Один Разовый секретный пароль может быть использован Клиентом для подтверждения только одной операции.

Клиенту необходимо внимательно изучать текст сообщений, содержащих Разовый секретный пароль, и в случае отличия описания совершаемой операции от реального намерения/волеизъявления Клиента – Клиенту рекомендуется не подтверждать операцию (не вводить Разовый секретный пароль).

8.3. Положения настоящего раздела применяются также для банковских карт, не имеющих материального носителя (виртуальных карт).

ПРАВИЛА работы в Сервисе «Интернет Платежи»

Сервис «Интернет платежи» (далее – Сервис) предоставляет Клиенту возможность с использованием Платежного кабинета совершать Распоряжения о переводе ЭДС и Распоряжения о возврате остатка ЭДС в адрес определенных Получателей, а также направлять в РНКО документы в электронном виде (далее - электронные документы) в случаях, предусмотренных Договором, на условиях, предусмотренных настоящими Правилами Сервиса и Договором.

Обмен электронными документами (в т.ч. ЭПД) в рамках Сервиса осуществляется на основании Правил электронного документооборота корпоративной информационной системы «BeSafe», которые размещены в сети Интернет по адресу www.besafe.ru. Присоединяясь к условиям Договора, предусматривающего возможность использования Сервиса, Клиент также присоединяется к Правилам электронного документооборота корпоративной информационной системы «BeSafe», расположенным в сети Интернет по адресу: www.besafe.ru. Совершение Клиентом с использованием Сервиса Распоряжений о переводе ЭДС и Распоряжений о возврате остатка ЭДС означает полное согласие Клиента с указанными правилами, действующими на момент совершения соответствующего распоряжения.

9. Доступ к СЕРВИСУ

9.1. Доступ Клиента к Сервису осуществляется после успешного прохождения Клиентом процедуры Идентификации, если возможность использования Сервиса предусмотрена Договором.

9.2. Идентификация Клиента в Сервисе производится при использовании Логина и Пароля для получения доступа в Платежный кабинет. РНКО и Клиент признают, что Логин и Пароль, используемые Клиентом при прохождении процедуры Идентификации, являются уникальными и подтверждают, что вход в Платежный кабинет и отдельные его разделы осуществляются Клиентом лично.

9.2.1. Первый вход в Платежный кабинет осуществляется с использованием EAN в качестве Логина. Вместо Пароля для первого входа в Платежный кабинет используется дата рождения Клиента, сообщенная Клиентом при заключении Договора. После ввода Логина и Пароля первый вход в Платежный кабинет подтверждается Клиентом Разовым секретным паролем. Если Клиент при заключении

Договора не сообщал дату рождения, для первого входа в Платежный кабинет вместо Пароля используется комбинация символов, высылаемая РНКО путем отправки Клиенту SMS-сообщения на Номер мобильного телефона после ввода Логина.

Пароль устанавливается Клиентом самостоятельно при первом входе в Платежный кабинет.

9.2.2. Возможность использования Клиентом Номера мобильного телефона в качестве Логина предоставляется исключительно Клиенту, использующему Карту клиента типа «Билайн», «Билайн World» или «Билайн World PayPass» после осуществления Клиентом первого входа в Платежный кабинет и выполнения им ряда последовательных действий, установленных инструкцией Интернет-сайта.

Один Номер мобильного телефона может использоваться в качестве Логина для доступа только в один Платежный кабинет. Клиент вправе отключить такую возможность для вышеуказанного Платежного кабинета и включить для другого Платежного кабинета, используемого также в рамках Договора при получении Клиентом второй/третьей Карты клиента «Билайн», «Билайн World» или «Билайн World PayPass», указав EAN новой Карты клиента при прохождении процедуры Идентификации и следуя инструкции Интернет-сайта.

Возможность использования в качестве Логина Номера мобильного телефона прекращается РНКО в одностороннем порядке в случаях:

1) замены в порядке, предусмотренном Договором, Карты клиента, EAN которой использовался при первом входе в Платежный кабинет;

2) замены Клиентом Номера мобильного телефона в порядке, предусмотренном Договором.

В случае замены Карты клиента или Номера мобильного телефона, в порядке предусмотренном Договором, возможность использования в качестве Логина Номера мобильного телефона устанавливается в порядке, аналогичном для первого входа в Платежный кабинет.

9.3. Мобильное приложение предоставляет возможность Клиенту пройти Идентификацию с использованием в качестве Логина совокупности EAN и Уникального идентификатора Мобильного приложения (далее – Мобильный логин), а также подтверждающего его Пароля, который устанавливается Клиентом самостоятельно. Мобильный логин может быть установлен и в дальнейшем использоваться Клиентом при получении доступа к Платежному кабинету исключительно посредством установленного на конкретное устройство Клиента Мобильного приложения.

Установка и отключение использования Мобильного логина, а также установка и изменение подтверждающего Мобильный логин Пароля осуществляются Клиентом после прохождения процедуры Идентификации, в соответствии с инструкциями в Мобильном приложении.

В случае отключения Клиентом по своей инициативе Идентификации с использованием ранее установленного Мобильного логина в Мобильном приложении Клиента, дальнейшая возможность Идентификации с использованием такого Мобильного логина прекращается. При этом Клиент вправе установить возможность Идентификации с использованием Мобильного логина заново. При замене Карты клиента, EAN которой используется в Мобильном логине, возможность Идентификации с использованием ранее установленного Мобильного логина прекращается.

9.4. Если Устройство оснащено сканером отпечатков пальцев и находится под управлением операционной системы iOS не ниже версии 8, при этом Клиент сохранил свой отпечаток пальца на Устройстве для его разблокировки, установил Мобильное приложение и в нем активировал функцию «Входить по Touch ID», Идентификация Клиента при входе в Мобильное приложение производится в следующем порядке:

Устройством запрашивается отпечаток пальца Клиента и в момент его сканирования происходит установление Клиента как владельца Устройства операционной системой. При положительном результате проверки происходит расшифровка и автоматический ввод Пароля, сохраненного в памяти Устройства в зашифрованном виде при включении функции, средствами Мобильного приложения.

Активация функции «Входить по Touch ID» возможна только для Клиентов, использующих Карту клиента типа «Билайн», или «Билайн World», или «Билайн World PayPass», или «Кукуруза», или «Кукуруза World», или «Кукуруза World PayPass».

РНКО не является разработчиком системы сканирования отпечатков пальцев, не получает и не обрабатывает биометрические персональные данные Клиента. Операционная система Устройства может допускать регистрацию нескольких владельцев по их отпечатку пальца. Установление Клиента как владельца Устройства по отпечатку пальца осуществляется исключительно средствами операционной системы такого Устройства, любое лицо, отпечаток пальца которого сохранен на Устройстве Клиента, и имеющее доступ к Устройству, имеет возможность успешно пройти Идентификацию.

При использовании возможности, указанной в настоящем пункте, Клиент обязан не допускать доступа третьих лиц к Устройству, а именно не устанавливать возможность использования отпечатка пальца на своем Устройстве для других лиц. При этом Клиент соглашается с тем, что риски наступления возможных негативных последствий, связанных с используемой технологией, которые могут возникнуть в результате действий третьих лиц (в том числе неправомерных действий третьих лиц, вызванных ненадлежащим соблюдением Клиентом настоящего пункта и пункта 9.6 настоящих Правил) возлагаются на Клиента.

9.5. Направление Клиентом РНКО электронного документа (в т.ч. ЭПД) подтверждается вводом Пароля при Идентификации и/или Разовым секретным паролем. Разовый секретный пароль направляется РНКО Клиенту в виде SMS-сообщения на Номер мобильного телефона, либо посредством PUSH-сообщения (если операция совершается с использованием Мобильного приложения и Клиент подключил возможность получения PUSH-сообщений) после запроса Клиента на предоставление Разового секретного пароля в Платежном кабинете. Один Разовый секретный пароль может быть использован Клиентом только один раз – при формировании одного электронного документа (в т.ч. ЭПД), за исключением случаев, указанных в настоящих Правилах работы в Сервисе.

Ввод Разового секретного пароля может не требоваться в случаях, определяемых РНКО. РНКО доводит данную информацию до Клиента путем отображения информации в Платежном кабинете при совершении Клиентом операции. Например, при направлении Клиентом Распоряжения о переводе ЭДС между своими Электронными кошельками, открытыми в рамках одного Договора в РНКО, при условии совпадения содержащихся в РНКО сведений о Клиенте (в т.ч. совпадения номера телефона), относящихся к этим Электронным кошелькам.

9.6. Клиент несет ответственность за сохранность и неизвестность третьим лицам Пароля и Разового секретного пароля, обязан хранить и использовать Пароль и Разовый секретный пароль способами, обеспечивающими невозможность его несанкционированного использования, в том числе – не передавать в пользование и не предоставлять для использования третьим лицам Номер мобильного телефона (SIM-карту), Устройство с установленным Мобильным приложением/Мобильное приложение (в особенности при активации функции «Входить по Touch ID») и незамедлительно уведомлять РНКО о Компрометации Пароля и/или Разового секретного пароля.

9.7. Клиент признает, что сформированные им после прохождения Идентификации и переданные в РНКО электронные документы (в т.ч. ЭПД), в том числе подтвержденные, в случаях предусмотренных Договором и настоящими Правилами, с помощью Разового секретного пароля:

- удовлетворяют требованию заключения сделки в простой письменной форме и влекут юридические последствия, аналогичные последствиям, порождаемым сделками, заключенными путем собственноручного подписания документов при физическом присутствии лиц, совершающих сделку;

- имеют равную юридическую и доказательственную силу аналогичным по содержанию и смыслу документам на бумажном носителе, составленным в соответствии с требованиями, предъявляемыми к документам такого рода, подписанным собственноручной подписью Клиента, и являются основанием для совершения РНКО Платежа в пользу соответствующих Получателей;

9.8. Доступ Клиента в Платежный кабинет может быть временно заблокирован без предварительного уведомления Клиента после трёхкратного последовательного ввода Клиентом неправильного Пароля. В данном случае происходит блокировка Логина на 180 секунд. После трех последовательных блокировок Логина обслуживание Клиента в Сервисе приостанавливается.

9.9. Для возобновления обслуживания Клиента в Сервисе Клиенту необходимо обратиться по телефону в Информационный центр. Сотрудник Информационного Центра после установления личности Клиента высылает новый временный Пароль SMS-сообщением на Номер мобильного телефона Клиента.

9.10. После трёхкратного последовательного ввода Клиентом неправильного Пароля, подтверждающего Мобильный логин, доступ к Платежному кабинету с использованием такого Мобильного логина прекращается. Клиент вправе заново установить использование Мобильного логина, следуя инструкциям в Мобильном приложении.

9.11. В случае наличия у РНКО оснований считать, что возможна Компрометация Пароля, Разового секретного пароля Клиента, обслуживание Клиента в Сервисе приостанавливается, о чем РНКО уведомляет Клиента не позднее следующего Рабочего дня после приостановления обслуживания в Сервисе.

9.12. Клиент вправе приостановить обслуживание в Сервисе, обратившись в РНКО с письменным заявлением или в Информационный центр с соответствующим заявлением в устной форме.

Клиент вправе подать РНКО заявление по установленной РНКО форме, определяющее параметры операций, которые могут осуществляться Клиентом в Платежном кабинете, путем его направления в Платежном кабинете (через сайт) либо почтовым отправлением посредством Почты России по почтовому адресу РНКО, указанному в Договоре. При невозможности однозначно установить из заявления волеизъявление Клиента по всем или некоторым параметрам (в силу некорректного заполнения полей заявления), РНКО исполняет заявление только в той части, в которой волеизъявление Клиента однозначно установлено.

9.13. Обслуживание Клиента в Сервисе может быть приостановлено для проведения профилактических работ и обновлений.

9.14. Обслуживание Клиента в Сервисе может быть приостановлено без предварительного уведомления Клиента в случае возникновения необходимости применения мер по управлению информационными и финансовыми рисками, когда непринятие указанных мер может повлечь возникновение угрозы безопасности работы Системы.

9.15. РНКО не возмещает любые убытки Клиента, возникшие в связи с приостановлением обслуживания Клиента в Сервисе, повлекшим невозможность формирования электронных документов (в т.ч. ЭПД).

9.16. При использовании Клиентом Сервиса РНКО вправе ограничить сумму и/или количество операций с ЭДС, а также ограничить список Получателей, в пользу которых Клиент может дать РНКО Распоряжение о переводе ЭДС и/или Распоряжение о возврате остатка ЭДС. Информацию об ограничениях, указанных в настоящем пункте, РНКО предоставляет при обращении Клиента в Информационный центр.

9.17. Установка и использование Мобильного приложения для доступа к Сервису запрещено, если Устройство Клиента работает или ранее работало в режиме суперпользователя (root). В случае нарушения Клиентом данного запрета Клиент принимает на себя риск убытков и иных неблагоприятных последствий в результате несанкционированного доступа третьих лиц к Платежному кабинету и информации о Разовых секретных паролях, направляемых на Номер мобильного телефона Клиента.

9.18. Держатели карт «Кукуруза», «Кукуруза World», «Кукуруза World Paypass» могут включить возможность использования Платежного кабинета через Интернет-сайт mybank.oplata.kykyryza.ru для просмотра и управления другими Электронными кошельками, открытыми в рамках Договора. Включение осуществляется, следуя инструкциям на сайте mybank.oplata.kykyryza.ru.

Клиенту предоставляется возможность перехода между сайтами mybank.oplata.kykyryza.ru и classic.oplata.kykyryza.ru для управления своими Электронными кошельками.

При переходе с сайта mybank.oplata.kykyryza.ru на сайт classic.oplata.kykyryza.ru для управления Электронным кошельком, соответствующим Карте клиента с EAN, отличным от EAN, с помощью которого проводилась Идентификация на сайте mybank.oplata.kykyryza.ru, Клиенту необходимо ввести Логин и Пароль для вышеуказанного Электронного кошелька на сайте classic.oplata.kykyryza.ru.

В иных случаях для перехода не требуется повторной Идентификации либо ввода Разового секретного пароля, а переход считается подтвержденным успешным прохождением Клиентом первоначальной процедуры Идентификации на сайте mybank.oplata.kykyryza.ru или classic.oplata.kykyryza.ru.

Просмотр и управление другими Электронными кошельками недоступны Клиенту, если он направил РНКО уведомление для блокировки Электронного средства платежа (которому соответствует Карта клиента, с помощью EAN которой осуществлялась Идентификация) в порядке, предусмотренном Договором, в связи его утратой или компрометацией, а также если такое Электронное средство платежа заблокировано по инициативе РНКО в предусмотренных Договором случаях.

Просмотр информации о других Электронных кошельках недоступен Клиенту, если истек Срок действия соответствующих им карт клиента или Клиент направил уведомление для блокировки соответствующих им Электронных средств платежа в порядке, предусмотренном Договором, в связи утратой или компрометацией Электронных средств платежа. При этом совершение операций с доступными Электронными кошельками возможно при условии, что соответствующие им Электронные средства платежа не заблокированы по инициативе РНКО или Клиента.

Включая данную возможность, Клиент осознает риск того, что при неисполнении/нарушении Клиентом Договора и/или настоящих Правил, доступ третьих лиц возможен также для управления другими Электронными кошельками Клиента и соглашается с тем, что риск убытков и иных неблагоприятных последствий в результате несанкционированного доступа третьих лиц для управления Электронными кошельками возлагается на Клиента.

10. Передача и исполнение Электронных платежных документов

10.1. Формирование и передача ЭПД Клиента.

10.1.1. Для формирования и передачи РНКО ЭПД в рамках Сервиса Клиентом заполняются специальные формы в соответствующем разделе Платежного кабинета.

10.1.2. Формирование ЭПД может осуществляться круглосуточно.

10.1.3. Дата и время регистрации ЭПД в Платежном кабинете подтверждает совершение операции с использованием Электронного средства платежа, факт поступления в РНКО ЭПД, а также исполнение РНКО обязанности по информированию Клиента о совершении операции с использованием Электронного средства платежа посредством Сервиса.

10.1.4. РНКО вправе отказать в исполнении ЭПД в следующих случаях:

- при отсутствии/недостаточности денежных средств (Остатка ЭДС) в Электронном кошельке Клиента для исполнения ЭПД Клиента, а также уплаты соответствующего Комиссионного сбора РНКО согласно Тарифному плану;
- если ЭПД не был подтвержден Клиентом, либо проверка Разового секретного пароля подтверждения ЭПД дала отрицательный результат.
- если сумма, указанная Клиентом в Распоряжении о переводе ЭДС или Распоряжении о возврате остатка ЭДС, в совокупности с суммой Комиссионного сбора превышает лимиты, установленные РНКО в соответствии с п. 9.16 Правил либо установленные в Договоре.
- отсутствует или технически прекращена возможность переводов через Платежный кабинет в пользу определенного Получателя.

10.2. Информация об ЭПД

10.2.1. Информация о переданных Клиентом ЭПД (совершении операций с ЭСП посредством Сервиса) отражается в Платежном кабинете.

10.2.2. Информация об исполнении РНКО переданных Клиентом ЭПД (распоряжений), операциях, совершенных в Электронном кошельке, о сумме Остатка ЭДС передается Клиенту в Отчете. Актуализация информации об Остатке ЭДС, может проводиться с задержкой до 1 (одного) Рабочего дня.

10.2.3. РНКО обязуется по запросу Клиента предоставить Клиенту документы на бумажном носителе, подтверждающие исполнение РНКО ЭПД Клиента.

10.2.4. РНКО обязана хранить полученные от Клиента ЭПД в течение предусмотренных законодательством России сроков для хранения аналогичных документов, составленных на бумажном носителе.

10.3. Исполнение ЭПД Клиента

10.3.1. Под исполнением РНКО ЭПД понимается исполнение распоряжения Клиента о переводе ЭДС или распоряжения Клиента о возврате Остатка ЭДС.

11. Формирование заранее данных Клиентом распоряжений

11.1. Клиент вправе с использованием специальных форм в соответствующем разделе Платежного кабинета заранее дать РНКО распоряжение в определенную календарную дату, или день недели, или при наступлении определенного события, являющегося основанием для осуществления перевода, осуществлять периодический перевод денежных средств определенному Получателю. Информация о таком распоряжении отображается Клиенту в Платежном кабинете до момента отмены распоряжения Клиентом или истечения срока для исполнения распоряжения, установленного Клиентом.

11.2. На основании распоряжения, переданного Клиентом в соответствии с п.11.1, в определенную календарную дату, или день недели, или при наступлении определенного события РНКО от имени Клиента самостоятельно составляет Распоряжение о возврате остатка ЭДС или Распоряжение о переводе ЭДС в адрес определенного Клиентом Получателя. Клиент вправе установить период времени, в течение которого такие распоряжения будут составляться РНКО.

Условия оказания Услуг «Автоплатеж-Билайн» предусмотрены Специальными условиями обслуживания или Условиями оказания Услуг «Автоплатеж-Билайн». Условия оказания Услуг «Автоплатеж-МТС», «Автоплатеж-МегаФон» предусмотрены Специальными условиями обслуживания.

11.3. Составление, а также изменение или отмена распоряжения, указанного в п. 11.1, подтверждается Клиентом Разовым секретным паролем. Удаление Клиентом из Платежного кабинета информации о заранее данных распоряжениях, исполнение которых невозможно в соответствии с п.10.1.4. настоящих Правил, не требует подтверждения Разовым секретным паролем.

11.4. РНКО вправе отказать в регистрации и исполнении распоряжения, составленного в соответствии с п.11.2, в случаях, предусмотренных п. 10.1.4 настоящих Правил, а также Договором.

12. Условия информационного обмена посредством PUSH-сообщений

12.1. Посредством PUSH-сообщений РНКО направляет Клиенту Разовый секретный пароль, предназначенный для подтверждения Клиентом операции, совершаемой с использованием Мобильного приложения, установленного на соответствующем Устройстве, а также иную конфиденциальную информацию в рамках Договора, в том числе являющуюся банковской тайной Клиента. Клиент соглашается на передачу вышеуказанной информации посредством технологии Apple Push Notification Service или Google Cloud Messaging. При этом Клиент осознает, что такие каналы передачи информации не всегда являются безопасными, и соглашается самостоятельно нести все риски, связанные с возможным нарушением конфиденциальности, возникающие вследствие использования таких каналов передачи информации, в том числе связанные с возможным получением информации третьим лицом.

12.2. Подключение возможности получения PUSH-сообщений:

12.2.1. Подключение возможности получения PUSH-сообщений осуществляется Клиентом посредством последовательного выполнения инструкций в Мобильном приложении, установленном на Устройство для соответствующего Электронного кошелька, и подтверждается вводом Разового секретного пароля в соответствии с правилами Сервиса «Интернет Платежи».

12.2.2 Факт ввода Клиентом Разового секретного пароля означает ознакомление Клиента с текстом настоящих Правил, полное и безусловное его согласие с настоящими Правилами, а также его согласие на передачу информации посредством технологии Apple Push Notification Service или Google Cloud Messaging. При этом Клиент осознает, что такие каналы передачи информации не всегда являются безопасными, и соглашается самостоятельно нести все риски, связанные с возможным нарушением конфиденциальности, возникающие вследствие использования таких каналов передачи информации, в том числе связанные с возможным получением информации третьим лицом.

12.2.3. Сведения о подключении возможности получения PUSH-сообщений доступны Клиенту в Платежном кабинете.

12.3. Порядок получения PUSH-сообщений:

12.3.1. PUSH-сообщения отправляются на одно Устройство с установленным Мобильным приложением, с использованием которого осуществлялось подключение возможности получения PUSH-сообщений.

12.3.2. Допускается получение на одно Устройство PUSH-сообщений для нескольких Электронных кошельков Клиента, в т.ч. открытых в рамках одного или нескольких Договоров о комплексном обслуживании клиента.

12.3.3. Для своевременного получения PUSH-сообщений Клиент обязуется обеспечить постоянное наличие у Устройства доступа к сети Интернет. При отсутствии подключения к сети Интернет доставка Клиенту PUSH-сообщений невозможна.

12.4. Отключение и прекращение получения PUSH-сообщений:

12.4.1. Клиент вправе отключить возможность получения PUSH-сообщений в Платежном кабинете.

12.4.2. РНКО прекращает отправку PUSH-сообщений на Устройство:

- при подключении возможности получения PUSH-сообщений для того же Электронного кошелька с использованием Мобильного приложения, установленного на другое Устройство.

- при удалении с Устройства, на которое осуществляется отправка PUSH-сообщений, Мобильного приложения.

12.4.3. В случае возникновения технических неисправностей или других обстоятельств, препятствующих направлению Клиенту PUSH-сообщений или обеспечению требуемого уровня безопасности, в том числе, в случае изменения действующего законодательства Российской Федерации, РНКО вправе в одностороннем порядке приостановить на неопределенный срок подключение и отправку PUSH-сообщений без предварительного уведомления Клиента.

12.4.4. При наступлении обстоятельств, указанных в пунктах 12.4.1-12.4.3 Правил, информационный обмен между РНКО и Клиентом осуществляется в порядке, установленном Договором.

12.5. Дополнительные условия:

12.5.1. Клиент признает, что РНКО не предоставляет услуги связи, технологию PUSH-сообщений и не несет ответственность за качество связи и несвоевременную доставку/недоставку PUSH-сообщений в случаях, когда передача информации Клиенту была невозможна по независящим от РНКО причинам, в том числе по вине операторов связи, провайдеров, Клиента или третьих лиц.

13. Условия использования AppleWatch

13.1. При наличии у Клиента, использующего Карту клиента типа «Билайн», «Билайн World» или «Билайн World PayPass», одновременно Устройства (iPhone 5 и выше) под управлением операционной системы iOS (от версии 8.2 и выше) и AppleWatch, Клиент имеет возможность установить на AppleWatch приложение для просмотра доступного Остатка ЭДС. Для этого Клиенту необходимо однозначно связать AppleWatch с Мобильным приложением на своем Устройстве через синхронизацию Устройства и AppleWatch, установив уникальный идентификатор AppleWatch (уникальная для каждой синхронизации Устройства с Мобильным приложением и AppleWatch последовательность латинских букв и цифр, которая формируется автоматически в момент синхронизации), используя средства операционной системы Устройства и Мобильное приложение.

13.2. Просмотр доступного Остатка ЭДС на AppleWatch возможен для Электронного кошелька, который управлялся посредством Мобильного приложения, с помощью которого было установлено приложение на AppleWatch. Для изменения Электронного кошелька, доступный остаток ЭДС которого отображается с помощью AppleWatch, необходимо пройти процедуру Идентификации для желаемого Электронного кошелька и следовать инструкциям Мобильного приложения.

13.3. Для просмотра доступного Остатка ЭДС в приложении AppleWatch необходимо наличие связи по каналу Bluetooth между синхронизированными Устройством и AppleWatch, ввода каких-либо паролей не требуется.

ПРАВИЛА работы в Сервисе «Мобильные платежи»

Настоящий Сервис предоставляет возможность Клиенту оплачивать услуги мобильной телефонной связи с использованием Номера мобильного телефона если возможность использования данного Сервиса предусмотрена Договором.

14. Порядок формирования распоряжений на оплату услуг мобильной связи

14.1. Для оплаты услуг мобильной телефонной связи по договору об использовании номера мобильного телефона Клиента Клиент:

14.1.1 отправляет с номера мобильного телефона на короткий номер, указанный в Договоре, SMS – сообщение, содержащее сумму перевода цифрами, например, «100».

Отправка указанного SMS-сообщения является направлением Клиентом Распоряжения о возврате остатка ЭДС, Получателем которого является соответствующий оператор мобильной связи, обслуживающий номер мобильного телефона Клиента, а также РНКО в части оплаты Комиссионного сбора.

14.2. Для оплаты услуг мобильной телефонной связи по договору об использовании других телефонных номеров Клиент отправляет с номера мобильного телефона Клиента на Короткий номер SMS – сообщение, содержащее номер мобильного телефона без префикса 8 и через пробел сумму перевода цифрами, например, «9000000000 100».

Отправка Клиентом указанного SMS-сообщения является направлением Клиентом РНКО Распоряжения о возврате остатка ЭДС, Получателем которого является соответствующий оператор мобильной связи, обслуживающий номер мобильного телефона, указанный в SMS-сообщении Клиента, а также РНКО в части оплаты Комиссионного сбора.

15. Прочие условия

15.1. Для обеспечения безопасности денежных средств Клиенту запрещается передавать другим лицам мобильный телефон с номером мобильного телефона Клиента.

15.2. Клиент обязан обеспечить наличие функции приёма и отправки SMS-сообщений на мобильном телефоне, номер которого указан Клиентом при заключении Договора.

15.3. Клиент соглашается на передачу Распоряжения о возврате остатка ЭДС и/или информации по каналам телефонной (сотовой) связи, осознавая, что такие каналы не всегда являются безопасными, и соглашается нести все риски, в том числе связанные с возможным нарушением конфиденциальности передаваемой таким образом информации, возникающие вследствие использования таких каналов передачи информации.

Председатель Правления *подпись* Г.М. Мац

«21» марта 2016 года