

*Правила действуют
с «11» апреля 2019 г.*

ПРАВИЛА использования Карты клиента и работы в Сервисе «Интернет Платежи»

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

Термины и определения

Google Pay – технология мобильных платежей от компании Google Ireland Limited, позволяющая Клиенту совершать операции с ЭДС при помощи Устройства Android в соответствии с разделом 10 настоящих Правил.

Приложение Google Pay – программное обеспечение, позволяющее Клиенту подключить Карту клиента к Google Pay (в частности, позволяющее создавать Токены и хранить информацию о них, а также информацию, позволяющую однозначно различить ту или иную Карту клиента: изображение карты, Реквизиты Карты клиента. Изображение Карты клиента в Приложении Google Pay может не соответствовать реальному дизайну Карты клиента). Приложение Google Pay разработано третьим лицом. Самостоятельная установка Клиентом Приложения Google Pay возможна исключительно в Google Play, где Приложение Google Pay распространяет организация Google LLC.

Apple Pay – технология мобильных платежей от корпорации APPLE DISTRIBUTION INTERNATIONAL, позволяющая Клиенту совершать операции с ЭДС при помощи Устройства Apple в соответствии с разделом 9 настоящих Правил.

Apple Wallet – предустановленная на Устройстве Apple программа, позволяющая создавать Токены и хранить информацию о них, а также информацию, позволяющую однозначно различить ту или иную Карту клиента: изображение карты, Реквизиты Карты клиента. Изображение Карты клиента в Apple Wallet может не соответствовать реальному дизайну Карты клиента. Apple Wallet разработана и распространяется третьими лицами.

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

Samsung Pay – технология мобильных платежей от компании Samsung Electronics Co., Ltd, позволяющая Клиенту совершать операции с ЭДС при помощи Устройства Samsung в соответствии с разделом 11 настоящих Правил.

Приложение Samsung Pay – разработанное и распространяемое правообладателем Samsung Electronics Co., Ltd предустановленное на Устройстве Samsung программное обеспечение, являющееся мобильным платежным сервисом, с помощью которого пользователь Устройства Samsung может хранить на своем Устройстве Samsung Токены, представляющие (заменяющие) Карты клиента с разрешения эмитента Карты клиента, и позволяющие безопасно использовать данные таких Токенов для совершения платежей или упрощения операций с Картами клиента. При этом по решению эмитента Карты клиента изображение Карты клиента в Приложении Samsung Pay может не соответствовать реальному дизайну Карты клиента.

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, а в случаях, определенных Правилами, также правильность, неизменность и целостность Электронного платежного документа.

Мобильное приложение – разработанное правообладателем ЗАО «ЦФТ» (адрес: 630559, Новосибирская область, Новосибирский р-н, р.п. Кольцово, д. 35) 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», «Карта Билайн» или «Ozon.Card» в зависимости от Карты клиента). В Google Play и AppStore приложение «Кукуруза» распространяет ООО «Сеть Связной» (Место нахождения: 125284, г. Москва, ул. Беговая, д.3, стр. 1, 36 этаж), приложение «Карта Билайн» – ПАО «ВымпелКом» (Место нахождения: 127083, г. Москва, ул. Восьмого Марта, дом 10, строение 14), а приложение «Ozon.Card» – ООО «Интернет Решения» (Место нахождения: 123112, г. Москва, Пресненская наб., д. 10, пом. I, эт. 41, комн. б) на основании соответствующих договоров с лицензиатом правообладателя (ЗАО «Биллингвый Центр», адрес: 630055, г. Новосибирск, ул. Мусы Джалиля, д. 11, оф. 218).

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 настоящими Правилами. 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.

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, Дополнительным электронным кошельком и Валютным 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 (код подтверждения) – 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, позволяющий организовать обмен документами в электронной форме (в том числе ЭПД) между РНКО и Клиентом в рамках Сервиса «Интернет Платежи». Доступ к функциональным возможностям Системы предоставлен РНКО в рамках использования РНКО Сервиса «ФАКТУРА.RU» (на основании ПРАВИЛ СЕРВИСА «ФАКТУРА.RU»).

Токен – цифровое представление Карты клиента, которое формируется по факту регистрации Карты клиента в Apple Wallet/Приложении Google Pay/Приложении Samsung Pay/Мобильном приложении, и которое хранится в зашифрованном виде в защищенном хранилище Устройства Apple/Устройства Android/Устройства Samsung.

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 – мобильное устройство Клиента (включая, но не ограничиваясь смартфон, коммуникатор, планшетный компьютер, носимое устройство и т.п.), работающее под управлением операционной системы iOS (версии не ниже iOS7), Android OS или Tizen.

Устройство, поддерживающее технологию Apple Pay, по тексту настоящих Правил именуется «Устройство Apple».

Устройство, поддерживающее технологию Google Pay, по тексту настоящих Правил именуется «Устройство Android».

Устройство, поддерживающее технологию Samsung Pay, по тексту настоящих Правил именуется «Устройство Samsung».

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

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, Устройства 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/ Устройства Apple/ Устройства Samsung/ Устройства Android и не допускать возможности использования Устройства с установленным Мобильным приложением/Устройства Samsung/ Устройства Apple/ Устройства Android третьими лицами.

1.16. Клиенту не рекомендуется устанавливать на свой компьютер, Устройство программное обеспечение из неофициальных источников. Рекомендуется использовать лицензионное программное обеспечение. При установке на Устройство программного обеспечения Клиенту рекомендуется проявлять внимательность, в частности перед установкой на Устройство Мобильного приложения и/или Приложения Google Pay сверять наименование организации, указанное в Google Play или AppStore в качестве распространителя программного обеспечения, с наименованием организации, указанным в настоящих Правилах.

1.17. В случае получения Клиентом предложения об установке любого программного обеспечения, якобы являющегося Мобильным приложением/ Приложением Google Pay/ Apple Wallet/ Приложением Samsung Pay или связанного с ним, из источников или от распространителей, отличных от указанных в настоящих Правилах, – Клиенту необходимо незамедлительно прекратить работу с таким источником и сообщить о произошедшем в Информационный центр.

1.18. На Устройство необходимо установить надежный пароль.

1.19. 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.

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

1.21. Клиент должен завершать каждый сеанс работы в Платежном кабинете путем нажатия соответствующей кнопки выхода из Платежного кабинета или закрытия страницы сайта, который использовался при работе с Платежным кабинетом, в том числе в случаях, когда Клиент делает перерыв в работе с Платежным кабинетом, вне зависимости от продолжительности перерыва. Не рекомендуется использовать функции, позволяющие сохранить (запомнить) пароли и прочую конфиденциальную информацию Клиента, а также запрещается оставлять без присмотра Клиента компьютер, Устройство с открытым на нем Платежным кабинетом, вход в который был ранее осуществлен Клиентом, и допускать доступ к ним третьих лиц.

1.22. Используя Google Pay/Apple Pay/Samsung Pay Клиент должен соблюдать конфиденциальность Токена, в частности, не копировать Токен, не совершать действий по расшифровыванию Токена, не предпринимать иные действия, в результате которых Токен может стать известным третьим лицам.

1.23. Порядок действий при выявлении операций, имеющих признаки их совершения без согласия Клиента:

1.23.1. При выявлении операции, содержащей признаки ее осуществления без согласия Клиента, РНКО приостанавливает исполнение соответствующего распоряжения Клиента, а также направляет Клиенту по Номеру мобильного телефона короткое текстовое сообщение (SMS-сообщение) о совершении вышеуказанных действий со ссылкой на рекомендации по снижению рисков повторного осуществления перевода денежных средств без согласия клиента, а также с инструкциями о действиях Клиента, необходимых для подтверждения возобновления исполнения распоряжения. Указанное SMS-сообщение также является уведомлением Клиента о совершении операции с использованием Электронного средства платежа.

Критерии наличия у операции признаков ее осуществления без согласия Клиента устанавливаются РНКО в одностороннем порядке и не подлежат опубликованию.

1.23.2. Одновременно с выполнением действий, предусмотренных п. 1.23.1 настоящих Правил, РНКО также приостанавливает возможность использования Электронного средства платежа, с использованием которого совершена операция, содержащая признаки ее осуществления без согласия Клиента. РНКО также вправе приостановить возможность использования иных Электронных средств платежа, используемых Клиентом в рамках того же Договора, в связи с наличием подозрений о возможности их неправомерного использования.

1.23.3. Если операция была действительно совершена без согласия Клиента, Клиент обязуется направить РНКО уведомление, предусмотренное Договором для случаев утраты/компрометации Электронного средства платежа, использования Электронного средства платежа без согласия Клиента. При невыполнении данной обязанности Клиент принимает на себя любые возможные риски и негативные последствия использования Электронного средства платежа без согласия клиента.

1.23.4. Если РНКО получена от Клиента информация о том, что операция действительно совершена без согласия Клиента, РНКО отказывает в исполнении соответствующего распоряжения.

1.23.5. При получении от Клиента подтверждения исполнения распоряжения РНКО незамедлительно возобновляет исполнение распоряжения Клиента, при получении от Клиента подтверждения возобновления использования Электронного средства платежа РНКО незамедлительно возобновляет использование Клиентом Электронного средства платежа. Указанные действия совершаются РНКО при условии, что Клиент не выполнял действия, предусмотренные п. 1.23.3 настоящих Правил.

1.23.6. При неполучении от Клиента подтверждения исполнения распоряжения РНКО возобновляет исполнение распоряжения и возможность использования Электронных средств платежа по истечении двух рабочих дней после дня совершения РНКО действий, предусмотренных п. 1.23.1 настоящих Правил.

2. Ответственность РНКО и Клиента. Доказательства в спорах

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/или Сервиса (в том числе убытки, понесенные в результате неправомерных действий третьих лиц), за исключением случаев, когда такие убытки были причинены Клиенту в результате неисполнения/ненадлежащего 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 (в том числе связанный с установкой на Устройство Клиента Мобильного приложения/ Приложения Google Pay/ Apple Wallet/ Приложения Samsung Pay из источников или от распространителей, отличных от указанных в настоящих Правилах).

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/Устройству Apple/Устройству Android/Устройству Samsung имеет только Клиент; Устройство с установленным Мобильным приложением/Мобильное приложение/Устройство Apple/Устройство Android/Устройство Samsung не используются третьими лицами. Также Клиент обязуется обеспечивать вышеуказанный режим использования Устройства с установленным Мобильным приложением/Мобильного приложения/Устройства Apple/Устройства Android/Устройства Samsung 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/Приложение Google Pay/ Apple Wallet/Приложение Samsung Pay, Мобильному приложению.

2.2.4. Клиент соглашается на передачу распоряжений и/или информации через сеть Интернет, в том числе с использованием Мобильного приложения/Приложения Google Pay/ Apple Wallet/Приложения Samsung Pay, 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.

Используя Google Pay/Apple Pay/Samsung Pay, а также Приложение Google Pay/Apple Wallet/Приложение Samsung Pay Клиент принимает на себя риск убытков и иных неблагоприятных последствий, связанный с возможным наличием уязвимостей в Google Pay/Apple Pay/Samsung Pay, а также в Приложении Google Pay/Apple Wallet/Приложении Samsung Pay. За негативные последствия, связанные с использованием Клиентом Google Pay/Apple Pay/Samsung Pay, а также Приложения Google Pay/Apple Wallet/Приложения Samsung Pay, РНКО ответственность не несет.

2.3. Клиент соглашается с тем, что в информационных системах РНКО автоматически производится регистрация всех действий Клиента с Картой клиента/Платежным кабинетом путем формирования специальных баз данных, признает достоверность сведений в

таких баз данных, а также, что информация из этих баз данных является надлежащим доказательством в спорах между РНКО и Клиентом.

ПРАВИЛА использования Карты клиента

3. Общие положения

3.1. Карта клиента может быть использована для совершения операций в торгово-сервисных предприятиях, в банковских учреждениях и устройствах самообслуживания (банкоматы, информационно-платежные терминалы) по правилам одной из международных платежных систем MasterCard Worldwide, VISA International или российских платежных систем «Золотая Корона», «МастерКард», «Виза».

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.

4.5. Во избежание использования Карты клиента другим лицом PIN-код необходимо хранить способами, обеспечивающими невозможность его несанкционированного использования, в том числе не сообщать PIN-код другим лицам, не вводить PIN-код при работе в сети Интернет.

4.6. При проведении операции с вводом PIN-кода необходимо прикрывать клавиатуру свободной рукой.

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.

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 одновременно.

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 в сети Интернет (на сайте третьего лица) 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 по Номеру мобильного телефона либо посредством PUSH-уведомления, направляемого на Устройство(-а) с установленным Мобильным приложением «Кукуруза» (если для оплаты используются Реквизиты Карты клиента типа «Кукуруза», «Кукуруза World» или «Кукуруза World PayPass») или на Устройство(-а) с установленным Мобильным приложением «Карта Билайн» (если для оплаты используются Реквизиты Карты клиента типа «Билайн», «Билайн World» или «Билайн World PayPass») или на Устройство (-а) с установленным Мобильным приложением «Ozon.Card» (если для оплаты используются Реквизиты Карты клиента «Ozon.Card»), 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 предоплаченных карт, не имеющих материального носителя (виртуальных карт).

9. ПРАВИЛА использования Карты клиента с применением Apple Pay

9.1. К Apple Pay могут быть подключены исключительно Карты клиента, перечисленные в Приложении №1 к настоящим Правилам.

Подключение Карты клиента к Apple Pay может осуществляться Клиентом через Мобильное приложение или через Apple Wallet.

9.1.1. С помощью Мобильного приложения подключение Карты клиента к Apple Pay осуществляется согласно инструкциям в Мобильном приложении и после Идентификации Клиента с использованием Логина и Пароля.

В Мобильном приложении необходимо выбрать Электронный кошелек, соответствующий Карте клиента, которая будет подключена к Apple Pay, нажать кнопку «Добавить в Apple Wallet»; подтвердить добавление Карты клиента; изучить настоящий раздел Правил и подтвердить свое безусловное согласие с ним; следовать дальнейшим информационным сообщениям в Мобильном приложении. Подробная информация об Apple Pay и Устройствах Apple, а также инструкции по использованию Apple Pay доступны на сайте <https://support.apple.com/ru-ru/HT204506>.

При подключении Карты клиента через Мобильное приложение Разовый секретный пароль по Контактному номеру телефона для подтверждения волеизъявления Клиента подключить Карту клиента к Apple Pay не направляется.

9.1.2. Для подключения Карты клиента к Apple Pay с помощью Apple Wallet Клиенту необходимо открыть приложение Apple Wallet, нажать кнопку «+» или «Добавить Карту» и следовать дальнейшим указаниям в Apple Wallet.

Клиент в обязательном порядке должен ввести Разовый секретный пароль, который поступит ему по номеру телефона, относящегося к добавляемой Карте клиента.

По факту успешной регистрации Карты клиента в Apple Wallet, Система Apple Pay направляет Клиенту соответствующее PUSH-уведомление.

9.2. Клиент вправе самостоятельно удалить Карту клиента, подключенную к Apple Pay посредством выбора соответствующей кнопки «Удалить карту» в Apple Wallet на Устройстве Apple, с использованием которого происходило подключение.

9.3. После завершения подключения Карты клиента к Apple Pay Клиент вправе производить платежи следующим образом:

9.3.1. осуществлять платежи через POS-терминал, установленный в ТСП MasterCard и оснащенный технологией бесконтактной связи, посредством поднесения Устройства Apple к POS-терминалу;

9.3.2. осуществлять платежи в мобильных приложениях на Устройстве Apple, поддерживающем расчеты через Apple Pay.

9.4. Если платеж совершен через POS-терминал, то подтверждение платежа может осуществляться с использованием Touch ID (сканер отпечатков пальцев) или Face ID (система распознавания лица). Подключение функции «Входить по Touch ID» или «Входить по Face ID» на Устройстве Apple осуществляется в порядке, предусмотренном в пп. 12.5.3 Правил. В случае если Touch ID или Face ID на Устройстве Apple отключен /не включен, Клиент перед тем, как совершить оплату через POS-терминал, активирует Apple Wallet с использованием пароля от Устройства Apple.

9.5. По завершении платежной операции в POS-терминале кассир должен выдать Клиенту чек. В чеке при совершении платежной операции с использованием Apple Pay помимо прочей информации указывается Токен, хранящийся в Устройстве Apple, с помощью которого произведена оплата.

9.6. В случае необходимости блокировки Карты, автоматически блокируются все Токены, соответствующие данной Карте на всех Устройствах Apple.

В случае утраты Устройства Apple, Клиенту необходимо обратиться в РНКО через Информационный Центр с целью блокировки Токена на данном Устройстве Apple.

9.7. В случае применения Apple Pay Клиент обязан соблюдать меры безопасности и защиты от мошенничества, предусмотренные настоящими Правилами.

9.8. С целью дополнительного обеспечения безопасности использования Apple Pay, Корпорация APPLE DISTRIBUTION INTERNATIONAL вправе устанавливать дополнительные условия использования Apple Pay, совершения платежей, информация о которых доводится до Клиента в Мобильном приложении/информационными сообщениями Apple Pay.

РНКО также вправе направлять Клиенту информационные сообщения, связанные с вопросами подключения или использования Apple Pay, информацию о доступности такой технологии для использования Клиентом.

9.9. Используя Apple Pay, Клиент дает РНКО поручение направлять в APPLE DISTRIBUTION INTERNATIONAL информацию об операциях, совершаемых Клиентом с использованием Apple Pay (в том числе, дату операции, валюту операции, наименование ТСП MasterCard, сумму операции, категорию и код отрасли).

Упомянутая в настоящем пункте информация об операциях направляется в APPLE DISTRIBUTION INTERNATIONAL с целью предоставления компании APPLE DISTRIBUTION INTERNATIONAL и ее аффилированным лицам возможности использовать такую информацию для:

- предоставления Клиенту истории операций такого Клиента, совершенных с использованием Apple Pay;
- обнаружения и устранения мошенничества;
- усовершенствования Apple Pay.

10. ПРАВИЛА использования Карты клиента с применением Google Pay

10.1. К Google Pay могут быть подключены исключительно Карты клиента, перечисленные в Приложении №1 к настоящим Правилам.

Подключение Карты клиента к Google Pay может осуществляться Клиентом с помощью Приложения Google Pay. Для этого Клиенту необходимо запустить на Устройстве Приложение Google Pay, нажать в нем кнопку «+», выбрать пункт «Добавить кредитную или дебетовую карту» и следовать дальнейшим указаниям в Приложении Google Pay. Подробная информация о Google Pay и Устройствах Android, а также инструкции по использованию Google Pay доступны на сайте <https://support.google.com/pay/answer/6224811?hl=ru>. Клиент в обязательном порядке должен ввести Разовый секретный пароль, который поступит ему по номеру телефона, относящегося к добавляемой Карте клиента.

10.2. Если у Клиента возникли какие-либо проблемы с подключением Карты клиента к Google Pay, Клиенту необходимо обратиться в Информационный центр.

10.3. Клиент вправе самостоятельно удалить Карту клиента, подключенную к Google Pay посредством выбора соответствующей кнопки «Удалить карту» в Приложении Google Pay на Устройстве Android, с использованием которого происходило подключение.

10.4. После завершения подключения Карты клиента к Google Pay Клиент вправе производить платежи следующим образом:

10.4.1. осуществлять платежи через POS-терминал, установленный в ТСП MasterCard и оснащенный технологией бесконтактной связи, посредством поднесения Устройства Android к POS-терминалу;

10.4.2. осуществлять платежи в мобильных приложениях на Устройстве Android, поддерживающем расчеты через Google Pay.

10.5. Если платеж совершен через POS-терминал, то подтверждение платежа может осуществляться с использованием сканера отпечатков пальцев или пароля (кода) для разблокировки Устройства Android.

10.6. По завершении платежной операции в POS-терминале кассир должен выдать Клиенту чек. В чеке при совершении платежной операции с использованием Google Pay помимо прочей информации указывается Токен, хранящийся в Устройстве Android, с помощью которого произведена оплата.

10.7. В случае необходимости блокировки Карты, автоматически блокируются все Токены, соответствующие данной Карте на всех Устройствах Android.

В случае утраты Устройства Android, Клиенту необходимо обратиться в РНКО через Информационный Центр с целью блокировки Токена на данном Устройстве Android.

10.8. В случае применения Google Pay Клиент обязан соблюдать меры безопасности и защиты от мошенничества, предусмотренные настоящими Правилами.

10.9. С целью дополнительного обеспечения безопасности использования Google Pay, компания Google Ireland Limited вправе устанавливать дополнительные условия использования Google Pay, совершения платежей, информация о которых доводится до Клиента информационными сообщениями Google Pay.

РНКО также вправе направлять Клиенту информационные сообщения, связанные с вопросами подключения или использования Google Pay, информацию о доступности такой технологии для использования Клиентом.

10.10. Компания Google Ireland Limited или РНКО может по своему усмотрению со своей стороны приостановить или прекратить предоставление Клиенту возможности осуществления оплат с применением Google Pay.

10.11. Используя Google Pay, Клиент дает РНКО поручение направлять в Google Ireland Limited информацию об операциях, совершаемых Клиентом с использованием Google Pay (в том числе, наименование ТСП MasterCard, город ТСП MasterCard, почтовый индекс ТСП MasterCard, сумму операции, дату операции, время операции, тип сделки, валюту операции, статус сделки, код категории отрасли, название категории отрасли, код отрасли и название отрасли).

Упомянутая в настоящем пункте информация об операциях направляется в Google Ireland Limited с целью предоставления компании Google Ireland Limited и ее аффилированным лицам возможности использовать такую информацию для:

- предоставления Клиенту истории операций такого Клиента, совершенных с использованием Google Pay;
- обнаружения и устранения мошенничества;
- создания отчетов об экономической эффективности Google Pay исключительно для использования внутри компании Google Ireland Limited;
- получения информации, необходимой для выполнения компанией Google Ireland Limited своих обязательств по отчетности перед третьими лицами касательно привлечения пользователей к Google Pay;
- усовершенствования Google Pay;
- рекламы Google Pay и проведения анализа распределения рекламных объявлений.

10.12. В случае использования Google Pay Клиент соглашается с тем, что РНКО может получать от Google Ireland Limited данные Устройства Android (в том числе марку/модель Устройства Android, IMEI Устройства Android и иные данные Устройства Android) в целях использования таких данных для технической поддержки Клиентов, разрешения споров, обнаружения и устранения мошенничества.

11. ПРАВИЛА использования Карты клиента с применением Samsung Pay

11.1. К Samsung Pay могут быть подключены исключительно Карты клиента, перечисленные в Приложении №1 к настоящим Правилам.

Подключение Карты клиента к Samsung Pay может осуществляться Клиентом с помощью Приложения Samsung Pay на Устройстве Samsung. Подробнее о Samsung Pay и Устройствах Samsung, а также инструкции по использованию Samsung Pay доступны на сайте <http://www.samsung.com/ru/apps/mobile/samsungpay/>.

Клиент в обязательном порядке должен ввести Разовый секретный пароль, который поступит ему по номеру телефона, относящегося к добавляемой Карте клиента.

11.2. Клиент вправе самостоятельно удалить Карту клиента, подключенную к Samsung Pay посредством выбора соответствующей кнопки «Удалить карту» в Приложении Samsung Pay на Устройстве Samsung, с использованием которого происходило подключение.

11.3. После завершения подключения Карты клиента к Samsung Pay Клиент вправе производить платежи следующим образом:

11.3.1. посредством поднесения Устройства Samsung к POS-терминалу, который установлен в ТСП MasterCard и который поддерживает оплату с использованием бесконтактной технологии «NFC» («Near Field Communication») и/или магнитной полосы;

11.3.2. в мобильных приложениях (на Устройстве Samsung), поддерживающих оплату покупок посредством Samsung Pay (где доступна кнопка «Оплатить Samsung Pay»);

11.3.3. на сайтах интернет-магазинов (через любой браузер), поддерживающих оплату покупок посредством Samsung Pay (где доступна кнопка «Оплатить Samsung Pay»).

Более подробная информация о способах оплаты доступна на сайте <http://www.samsung.com/ru/apps/mobile/samsungpay/>.

11.4. Для совершения каждого отдельного платежа посредством Samsung Pay требуется успешная аутентификация Клиента в Приложении Samsung Pay посредством радужки глаза, отпечатка пальца или пин-кода Приложения Samsung Pay (в зависимости от технических возможностей используемого Клиентом Устройства Samsung). В случае неуспешной аутентификации Клиента в Приложении Samsung Pay платеж совершен быть не может (данные для совершения платежа не передаются с Устройства Samsung).

При этом если платеж совершается посредством POS-терминала, то вместо ввода PIN-кода Карты клиента на POS-терминале подтверждение платежа может осуществляться посредством аутентификации Клиента в Приложении Samsung.

11.5. По завершении платежной операции, совершенной посредством Samsung Pay, Клиент получает чек (так же как при совершении платежа с использованием Карты клиента). При этом в чеке помимо прочей информации вместо последних 4-х (четырех) цифр номера Карты клиента указываются последние 4 (четыре) цифры номера соответствующего Токена. Последние 4 цифры Токена на чеке можно сравнить с информацией в Приложении Samsung Pay, относящейся к соответствующей Карте клиента (смотрите «Последние 4 цифры для кассира» под изображением карты).

11.6. В случае блокировки Карты клиента, автоматически блокируются все Токены, соответствующие данной Карте на всех Устройствах Samsung.

В случае утраты Устройства Samsung, Клиенту необходимо обратиться в РНКО через Информационный Центр с целью блокировки Токена на данном Устройстве Samsung, а также воспользоваться сервисом «Samsung Find My Mobile» («Найти мое мобильное устройство»), чтобы заблокировать или удалить все данные Samsung Pay с Устройства Samsung (<https://findmymobile.samsung.com/>).

11.7. В случае применения Samsung Pay Клиент обязан соблюдать меры безопасности и защиты от мошенничества, предусмотренные настоящими Правилами.

11.8. С целью дополнительного обеспечения безопасности использования Samsung Pay, Samsung Electronics Co., Ltd вправе устанавливать дополнительные условия использования Samsung Pay, совершения платежей, информация о которых доводится до Клиента информационными сообщениями Samsung Pay.

РНКО также вправе направлять Клиенту информационные сообщения, связанные с вопросами подключения или использования Samsung Pay, информацию о доступности такой технологии для использования Клиентом.

11.9. РНКО может по своему усмотрению со своей стороны приостановить или прекратить предоставление Клиенту возможности осуществления оплат с применением Samsung Pay.

11.10. В случае использования Samsung Pay Клиент соглашается с тем, что РНКО может получать от Samsung Electronics Co., Ltd данные Устройства Samsung (такие как марка/модель Устройства Samsung, и иные данные Устройства Samsung) в целях использования таких данных для технической поддержки Клиентов, разрешения споров, обнаружения и устранения мошенничества.

ПРАВИЛА работы в Сервисе «Интернет Платежи»

Сервис «Интернет платежи» (по тексту документа – Сервис) предоставляет Клиенту возможность с использованием Платежного кабинета совершать Распоряжения о переводе ЭДС и Распоряжения о возврате остатка ЭДС в адрес определенных Получателей, направлять в РНКО документы в электронном виде (далее - электронные документы) в случаях, предусмотренных Договором, на условиях, предусмотренных настоящими Правилами Сервиса и Договором, просматривать историю операций, формировать Отчет об операциях, формировать шаблоны распоряжений, устанавливать лимиты на проведение операций, осуществлять иное информационное взаимодействие. Осуществляя вход в Платежный кабинет, Клиент каждый раз соглашается с действующей в момент такого входа редакцией Правил Сервиса.

Функционал Платежного кабинета, доступ к которому осуществляется с использованием Мобильного приложения, может отличаться от функционала Платежного кабинета, доступ к которому осуществляется с использованием Интернет-сайта, указанного в Договоре, а также может зависеть от технических характеристик Устройства. Сведения о возможностях и особенностях использования конкретного Платежного кабинета представлены в Платежном кабинете в виде инструкций и подсказок.

Поскольку функционал Сервиса постоянно дополняется и обновляется, его функциональные возможности могут периодически изменяться без предварительного уведомления Клиента. РНКО вправе при необходимости по собственному усмотрению приостановить или прекратить возможность использования Сервиса (или каких-либо отдельных функций в рамках Сервиса) всем Клиентам или отдельному Клиенту без предварительного уведомления, в том числе в случае нарушения Клиентом условий Договора. 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.

12. Доступ к СЕРВИСУ, работа в СЕРВИСЕ

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

12.2. РНКО и Клиент признают, что Логин и Пароль, используемые Клиентом при прохождении процедуры Идентификации, являются уникальными.

12.3. Первый вход в Платежный кабинет осуществляется с использованием EAN в качестве Логина. После ввода Логина Клиент вводит Разовый секретный пароль, направленный РНКО Клиенту в виде SMS-сообщения по Номеру мобильного телефона. Пароль устанавливается Клиентом самостоятельно при первом входе в Платежный кабинет.

12.4. Использование Номера мобильного телефона в качестве Логина:

12.4.1. Клиенту, использующему Карту клиента типа «Билайн», «Билайн World» или «Билайн World PayPass» или Карту клиента типа «Кукуруза», «Кукуруза World», «Кукуруза World PayPass» или Карту клиента «Ozon.Card», после осуществления Клиентом первого входа в Платежный кабинет через соответствующий типу Карты клиента интернет-сайт или Мобильное приложение, предоставляется возможность использования в качестве Логина Номера мобильного телефона.

Исключение составляют случаи, когда возможность входа по Номеру мобильного телефона уже предоставлена Клиенту, в том числе с использованием другого Логина, либо Клиент запретил использование в качестве Логина Номера мобильного телефона.

Клиент вправе настроить возможность использования в качестве Логина Номера мобильного телефона или отключить ее, следуя при этом соответствующим инструкциям в Платежном кабинете.

12.4.2. В случае изменения Номера мобильного телефона, используемого в качестве Логина для входа в Платежный кабинет, Логин Клиента будет соответствовать измененному Номеру мобильного телефона, при этом замена ранее установленного Клиентом Пароля не требуется.

12.4.3. Для доступа к Платежному кабинету Клиент применяет один Пароль при использовании в качестве Логина как EAN Карты Клиента, так и Номера мобильного телефона.

12.4.4. В случае замены в порядке, предусмотренном Договором, Карты клиента, EAN которой использовался при первом входе в Платежный кабинет, Клиент осуществляет вход в Платежный кабинет с использованием в качестве Логина EAN замененной Карты клиента. Для последующих входов в Платежный кабинет Клиент вправе использовать в качестве Логина Номер мобильного телефона.

12.5. Особенности входа в Платежный кабинет через Мобильное приложение:

12.5.1. При входе в Платежный кабинет через Мобильное приложение Логин сохраняется автоматически и на экране Устройства не отображается.

12.5.2. Мобильное приложение предоставляет Клиенту возможность пройти Идентификацию с использованием Пароля, состоящего из 4 (четырёх) цифр (далее по тексту – «Короткий Пароль»). Короткий Пароль устанавливается Клиентом самостоятельно с использованием соответствующего функционала Мобильного приложения.

Короткий Пароль может быть установлен и в дальнейшем использован Клиентом при получении доступа к Платежному кабинету исключительно посредством установленного на конкретное устройство Клиента Мобильного приложения. При этом в качестве Логина в таком случае используется совокупность EAN или Номера мобильного телефона и соответствующего Уникального идентификатора Мобильного приложения (далее по тексту – «Мобильный логин»).

При последующих входах в Платежный кабинет с использованием Мобильного приложения на этом же Устройстве требуется ввести только Короткий Пароль. Мобильный логин сохраняется автоматически и на экране Устройства не отображается.

Установка, изменение и отключение Короткого 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 Короткого Пароля в Мобильном приложении Клиента, дальнейшая возможность Идентификации с использованием такого Короткого Пароля прекращается. При этом Клиент вправе установить возможность Идентификации с использованием Короткого Пароля заново.

При замене Карты клиента, EAN которой используется в Мобильном логине, возможность Идентификации с использованием Короткого Пароля, ранее установленного для такого Мобильного логина, прекращается.

12.5.3. Если Устройство оснащено сканером отпечатков пальцев или системой распознавания лица и находится под управлением операционной системы iOS не ниже версии 8 либо операционной системы Android не ниже версии 2.7, при этом Клиент сохранил свой отпечаток пальца или структурную карту лица на Устройстве для его разблокировки, установил Мобильное приложение и в нем активировал функцию «Входить по Touch ID» или «Входить по Face ID», Идентификация Клиента при входе в Мобильное приложение производится в следующем порядке:

Устройством запрашивается отпечаток пальца Клиента или структурная карта лица 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» или «Входить по Face ID» возможна только для Клиентов, использующих Карту клиента типа «Билайн», или «Билайн World», или «Билайн World PayPass» (для Устройств с iOS или Android); или «Кукуруза», или «Кукуруза World», или «Кукуруза World PayPass» (для Устройств с iOS или Android); или «Ozon.Card».

РНКО не является разработчиком системы сканирования отпечатков пальцев и системы распознавания лица, не получает и не обрабатывает биометрические персональные данные Клиента. Операционная система Устройства может допускать регистрацию нескольких владельцев по их отпечатку пальца или структурной карте лица. Установление Клиента как владельца Устройства по отпечатку пальца или структурной карте лица осуществляется исключительно средствами операционной системы такого Устройства, любое лицо, отпечаток пальца или структурная карта лица 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 или структурной карты лица 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 12.7 настоящих Правил) возлагаются на Клиента.

12.6. Направление Клиентом РНКО электронного документа (в т.ч. ЭПД) подтверждается одним из следующих способов, определяемых РНКО:

1) вводом Пароля при Идентификации и Разовым секретным паролем, если в Платежном кабинете требуется его ввод. Разовый секретный пароль направляется РНКО Клиенту в виде SMS-сообщения по Номеру мобильного телефона либо в PUSH-уведомлении после запроса Клиента о предоставлении 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.

2) нажатием в Платежном кабинете предлагаемой Сервисом соответствующей кнопки (например, «подтвердить», «подписать» и т.д.), в результате чего электронному документу (в т.ч. ЭПД) присваивается уникальный набор символов, сформированный для Клиента при Идентификации (идентификатор сессии). Ввод Разового секретного пароля не требуется.

РНКО доводит до Клиента информацию об используемом способе подтверждения Клиентом направления электронного документа (в т.ч. ЭПД) путем отображения информации в Платежном кабинете при совершении операции.

12.7. 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» или «Входить по Face ID») и незамедлительно уведомлять РНКО о Компрометации Пароля и/или Разового секретного пароля.

12.8. Клиент признает, что сформированные им после прохождения Идентификации и переданные в РНКО электронные документы (в т.ч. ЭПД), в том числе подтвержденные способами, предусмотренными п. 12.6 Правил:

- 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 надлежащим и достаточным основанием для совершения РНКО Платежа в пользу соответствующих Получателей;

12.9. 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.

12.10. 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 по Номеру мобильного телефона Клиента.

12.11. 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.

12.12. 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.

12.13. 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 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.

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

12.15. 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.

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

12.17. 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.

12.18. 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 по Номеру мобильного телефона Клиента.

12.19. Держатели Карт клиента типа «Кукуруза», «Кукуруза World», «Кукуруза World PayPass», держатели Карт клиента типа «Билайн», «Билайн World», «Билайн World PayPass», держатели Карт KARI100, держатели Карт ИОН100, а также держатели Карт клиента, индивидуализированных товарным знаком «ДОМАШНИЕ ДЕНЬГИ», товарным знаком «ОТЛИЧНЫЕ НАЛИЧНЫЕ» или товарным знаком «mycard», имеют возможность использовать один Логин для доступа в Платежный кабинет через соответствующий Карте клиента интернет-сайт oplata.kykyryza.ru, bank.beeline.ru, oplata.kari.com, pay.khclub.ru, pay.domadengi.ru, pay.otlnal.ru или pay.mycard.ru, либо через соответствующее Карте клиента Мобильное приложение «Кукуруза» или «Карта Билайн» для просмотра и управления всеми Электронными кошельками, открытыми в рамках Договора (за исключением Электронных кошельков, соответствующих Картам KARI15 или Картам ИОН15), при условии, что для них Клиентом используется одинаковый Номер мобильного телефона. Для Платежного кабинета, доступ к которому осуществляется через сайт oplata.kykyryza.ru, bank.beeline.ru, oplata.kari.com, pay.khclub.ru, pay.domadengi.ru, pay.otlnal.ru или pay.mycard.ru, либо через Мобильное приложение «Кукуруза» или «Карта Билайн», подключение осуществляется автоматически при первом входе в Платежный кабинет.

Мобильные приложения «Кукуруза» и «Карта Билайн» предоставляют Клиенту возможность одновременно для всех Электронных кошельков, открытых в рамках Договора, нажатием соответствующей кнопки одновременно отключить: Идентификацию с использованием ранее установленного Клиентом Пароля, подтверждающего Мобильный логин; установленные Клиентом ограничения на сумму и/или количество операций с ЭДС; информирование PUSH-уведомлениями с целью получения Информационных уведомлений; функцию бесконтактной оплаты в Мобильном приложении (при ее наличии), функцию «Входить по Touch ID»/«Входить по Face ID» (при ее наличии).

12.20. Просмотр и управление всеми Электронными кошельками недоступны Клиенту, если он направил РНКО уведомление для блокировки Электронного средства платежа (которому соответствует Карта клиента, с помощью EAN которой, как Логина, 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.

Осуществляя вход в Платежный кабинет, Клиент осознает риск того, что при неисполнении/нарушении Клиентом Договора и/или настоящих Правил, доступ третьих лиц возможен для управления всеми 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.

12.21. Держатель Карты клиента «Ozon.Card», если он направил РНКО уведомление о блокировке Электронного средства платежа (которому соответствует Карта клиента «Ozon.Card», с помощью EAN которой, как Логина, 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, имеет возможность осуществить вход в Платежный кабинет с целью подачи заявлений в РНКО.

12.22. Валютные электронные кошельки могут быть созданы по запросу Клиента в Платежном кабинете, доступ к которому осуществляется с сайтов oplata.kykyrgyza.ru, bank.beeline.ru, card.ozon.ru. Для создания Валютного электронного кошелька Клиенту необходимо войти в Платежный кабинет по Логину действующей Карты клиента. В Валютный электронный кошелек при его создании передаются сведения о Клиенте, соответствующие Электронному кошельку с таким Логинем.

Управление Валютными электронными кошельками доступно Клиенту при получении доступа к Платежному кабинету под любым из Логинов Клиента, которому соответствует такой же Контактный номер телефона.

13. Передача и исполнение Электронных платежных документов

13.1. Формирование и передача ЭПД Клиента.

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

13.1.2. Формирование ЭПД может осуществляться круглосуточно.

13.1.3. 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.

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

- при отсутствии/недостаточности денежных средств (Остатка ЭДС) в Электронном кошельке/Валютном 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. 12.17 Правил либо установленные в Договоре.
- отсутствует или технически прекращена возможность переводов через Платежный кабинет в пользу определенного Получателя
- иных случаях, предусмотренных Договором.

13.2. Информация об ЭПД

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

13.2.2. Информация об исполнении РНКО переданных Клиентом ЭПД (распоряжений) и иных 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 (с момента исполнения РНКО соответствующего распоряжения/совершения в Электронном кошельке соответствующей операции).

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

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

13.3. Исполнение ЭПД Клиента

13.3.1. Под исполнением РНКО ЭПД понимается исполнение Распоряжения о переводе ЭДС или Распоряжения о возврате Остатка ЭДС.

14. Исполнение заранее данных Клиентом распоряжений

14.1. В случае, если Клиентом с использованием специальных форм в соответствующем разделе Платежного кабинета заранее дано РНКО распоряжение при наступлении определенного события, являющегося основанием для осуществления перевода, осуществлять периодический перевод денежных средств определенному Получателю (в целях оплаты услуг оператора мобильной связи), РНКО на основании такого распоряжения и при наступлении определенного события от имени Клиента самостоятельно составляет Распоряжение о возврате остатка ЭДС в адрес определенного Клиентом Получателя.

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

14.2. Отмена распоряжения, указанного в п. 14.1, производится Клиентом путем обращения в Информационный центр.

Составление новых, а также изменение уже данных распоряжений не допускается.

14.3. РНКО вправе отказать в исполнении распоряжения в случаях, предусмотренных п. 13.1.4 настоящих Правил, а также Договором.

15. Уведомления

15.1. Информирование клиента о совершенных операциях (в том числе об операциях пополнения Электронного кошелька, операциях расходования ЭДС, возникновении у Клиента задолженности перед РНКО и другие уведомления (далее – Информационные уведомления)) осуществляется путем отображения информации в Платежном кабинете, а также РНКО вправе дополнительно информировать Клиента путем направления SMS-сообщения по Номеру мобильного телефона или направления PUSH-уведомлений в Мобильном приложении в порядке, предусмотренном Договором.

Предоставление Клиенту Разового секретного пароля осуществляется РНКО посредством направления SMS-сообщений по Номеру мобильного телефона или PUSH-уведомлений в Мобильном приложении.

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.

15.2. Подключение информирования PUSH-уведомлениями:

15.2.1. На устройство с установленным Мобильным приложением «Кукуруза» (версия приложения для Android – 2.4.1 и ниже, версия приложения для iOS – 1.17.1 и ниже), Мобильным приложением «Карта Билайн» (версия приложения для Android – 1.11.2 и ниже, версия приложения для iOS – 1.15 и ниже) подключение информирования PUSH-уведомлениями с целью получения Информационных уведомлений подтверждается вводом Разового секретного пароля. Клиент вправе изменить способ получения уведомлений, следуя инструкциям в Платежном кабинете.

15.2.2. На устройство с установленным Мобильным приложением «Кукуруза» (версия приложения для Android – 2.5 и выше, версия приложения для iOS – 2.0 и выше), с установленным Мобильным приложением «Карта Билайн» (версия приложения для Android – 3.0 и выше, версия приложения для iOS – 3.0 и выше) или с установленным Мобильным приложением «Ozon.Card» подключение информирования:

- PUSH-уведомлениями с целью получения Информационных уведомлений происходит после первого успешного входа Клиента в Платежный кабинет с использованием Мобильного приложения. При этом Информационные уведомления направляются одновременно на все Устройства, где Клиентом был совершен вход с использованием Мобильного приложения. Клиент вправе изменить способ получения Информационных уведомлений, следуя инструкциям в Платежном кабинете.

- PUSH-уведомлениями с целью получения Разовых секретных паролей, подтверждается Клиентом путем ввода Разового секретного пароля, направляемого посредством SMS-сообщения по Номеру мобильного телефона при совершении первой операции в Мобильном приложении. При отказе от получения таких PUSH-уведомлений (не введен Разовый секретный пароль), возможность совершения операций с Остатком ЭДС через МП недоступна. Изменение способа получения уведомлений с Разовыми секретными паролями не предусмотрено.

15.3. Установка и использование Клиентом Мобильного приложения означает полное согласие на информирование Клиента PUSH-уведомлениями, в том числе о Разовых секретных паролях.

15.4. Факт ввода Клиентом Разового секретного пароля означает ознакомление Клиента с текстом настоящих Правил, полное и безусловное его согласие с настоящими Правилами.

15.5. Информирование PUSH-уведомлениями осуществляется для Электронного кошелька, которому соответствует Логин, использованный при подключении информирования.

15.6. В случае утраты Устройства, Клиент обязан отключить информирование PUSH-уведомлениями на Устройстве путем обращения в Информационный Центр, а также предпринять действия по блокировке Электронного средства платежа в соответствии с условиями Договора.

15.7. РНКО вправе прекратить подключение информирования PUSH-уведомлениями и отправку PUSH-уведомлений в одностороннем порядке, в т.ч. случае возникновения технических неисправностей или других обстоятельств, препятствующих направлению Клиенту PUSH-уведомлений или обеспечению требуемого уровня безопасности, включая случаи изменения действующего законодательства Российской Федерации, без предварительного уведомления Клиента. В данном случае информационный обмен между РНКО и Клиентом осуществляется в порядке, установленном Договором.

15.8. Клиент признает, что РНКО не предоставляет услуги связи, технологию PUSH-уведомлений и не несет ответственность за качество связи и несвоевременную доставку/недоставку PUSH-уведомлений 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.

Председатель Правления *подпись* Г.М. Мац
«11» апреля 2019 года

ПЕРЕЧЕНЬ
Карт клиента, которые могут быть подключены к технологиям мобильных платежей

Технология мобильных платежей	Тип Карты клиента, которая может быть подключена к технологии мобильных платежей
Apple Pay	<ol style="list-style-type: none"> 1. Карты клиента типа «Билайн», «Билайн World», «Билайн World PayPass»; 2. Карты клиента типа «Кукуруза», «Кукуруза World», «Кукуруза World PayPass»; 3. Карты KARI15, Карты KARI100; 4. Карты ИОН15, Карты ИОН100; 5. Карты клиента «Ozon.Card»; 6. Карты клиента с логотипом Международной платежной системы MasterCard Worldwide, перечисленные на сайте rnko.ru в разделе «Карты – Карта микрофинансовой организации» (доступном по адресу http://rnko.ru/individualcards/Pages/default.aspx); 7. Карты клиента с логотипом Международной платежной системы MasterCard Worldwide, перечисленные на сайте rnko.ru в разделе «Карты – Корпоративная подарочная» (доступном по адресу http://rnko.ru/individualcards/Pages/default.aspx); 8. Карты клиента с логотипом Международной платежной системы MasterCard Worldwide, перечисленные на сайте rnko.ru в разделе «Карты – Виртуальная подарочная» (доступном по адресу http://rnko.ru/individualcards/Pages/default.aspx).
Google Pay	<ol style="list-style-type: none"> 1. Карты клиента типа «Билайн», «Билайн World», «Билайн World PayPass»; 2. Карты клиента типа «Кукуруза», «Кукуруза World», «Кукуруза World PayPass»; 3. Карты KARI15, Карты KARI100; 4. Карты ИОН15, Карты ИОН100; 5. Карты ТНК15, Карты ТНК100; 6. Карты клиента «Ozon.Card»; 7. Карты клиента с логотипом Международной платежной системы MasterCard Worldwide, перечисленные на сайте rnko.ru в разделе «Карты – Корпоративная подарочная» (доступном по адресу http://rnko.ru/individualcards/Pages/default.aspx); 8. Карты клиента с логотипом Международной платежной системы MasterCard Worldwide, перечисленные на сайте rnko.ru в разделе «Карты – Карта микрофинансовой организации» (доступном по адресу http://rnko.ru/individualcards/Pages/default.aspx); 9. Карты клиента с логотипом Международной платежной системы MasterCard Worldwide, перечисленные на сайте rnko.ru в разделе «Карты – Корпоративная карта питания» (доступном по адресу http://rnko.ru/individualcards/Pages/default.aspx); 10. Карты клиента с логотипом Международной платежной системы MasterCard Worldwide, перечисленные на сайте rnko.ru в разделе «Карты – Виртуальная подарочная» (доступном по адресу http://rnko.ru/individualcards/Pages/default.aspx).
Samsung Pay	<ol style="list-style-type: none"> 1. Карты клиента типа «Кукуруза», «Кукуруза World», «Кукуруза World PayPass»; 2. Карты клиента типа «Билайн», «Билайн World», «Билайн World PayPass».

Председатель Правления *подпись* Г.М. Мац
«11» апреля 2019 года