РНКО ПЛАТЕЖНЫЙ ЦЕНТР

Правила действуют
с «16» июля 2022 года

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 – Договор). Неотъемлемой частью Правил является Приложение №1 - Условия использования Карты клиента при осуществлении операции с использованием Платежных приложений Apple Wallet, Google Pay, Samsung Pay, Mir Pay (далее – Приложение №1).

Термины и определения

Идентификация – процедура получения Клиентом доступа к Сервису «Интернет Платежи», осуществляемая с использованием Логина и Пароля либо, если это специально предусмотрено Договором, с использованием Логина и Разового секретного 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) платежное приложение, 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 «Связной Плюс» (ранее использовалось наименование «Кукуруза»), «Карта Билайн», «Ozon.Card» или «Денежные переводы» в зависимости от Карты клиента). Поставщиком платежного приложения является ЗАО «ЗОЛОТАЯ КОРОНА» (Место нахождения: 630102, город Новосибирск, улица Кирова, 86) на основании соответствующего договора с РНКО. В Google Play и AppStore приложение «Денежные переводы» распространяет поставщик платежного приложения (название магазина в Google Play - KoronaPay, название магазина в AppStore – Золотая Корона), на основании соответствующих договоров с поставщиком платежного приложения приложение «Связной Плюс» распространяет ООО «Сеть Связной» (Место нахождения: 123007, город Москва, проезд Хорошёвский 2-й, дом 9, корпус 2, этаж 5, комн 4; название магазина в Google Play - LLC «Svyaznoy Chain»; название магазина в AppStore - Svyaznoy Chain LLC), приложение «Карта Билайн» – ПАО «ВымпелКом» (Место нахождения: 127083, г. Москва, ул. Восьмого Марта, дом 10, строение 14; название магазина в Google Play - ПАО «ВымпелКом»; название магазина в AppStore - PJSC VimpelCom). Мобильное приложение «Ozon.Card» в Google Play и AppStore распространяло ООО «Интернет Решения» (Место нахождения: 123112, г. Москва, Пресненская наб., д. 10, пом. I, эт. 41, комн. 6; название магазина в Google Play - Internet Solutions LLC; название магазина в AppStore - OZON.ru). С «11» июля 2022 года возможность установить Мобильное приложение «Ozon.Card» Клиенту не предоставляется.

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 лицевой/обратной стороне Карты клиента, и, если допускается Правилами, Контактный номер телефона. Для Мобильного приложения в качестве Логина используется совокупность EAN и Уникального идентификатора Мобильного приложения либо качестве Логина может использоваться только Контактный номер телефона, если это прямо предусмотрено настоящими Правилами. Допускается наличие у Клиента более одного Логина. В таком случае, действие, совершенное Клиентом под любым из Логинов, имеет равную силу и влечет одинаковые юридические последствия.

Контактный номер 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 (кроме случаев, когда использование Пароля не предусмотрено Договором или настоящими Правилами), 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», или Сайта для управления услугами. 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».

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: часы, браслет, кольцо 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».

Устройство, поддерживающее технологию Mir Pay, по тексту настоящих правил именуется «Устройство Mir Pay».

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/Разового секретного 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.

PUSH-уведомление – короткое текстовое уведомление, всплывающее на экране Устройства с установленным Мобильным приложением. PUSH-уведомления могут поступать исключительно при наличии доступа к сети Интернет и при условии разрешения Клиентом получения уведомлений в настройках Устройства.

Термины, не определенные в настоящих Правилах, применяются в том значении, в котором они определены в Договоре или Приложении №1. 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. **Меры безопасности, предпринимаемые Клиентом при использовании Карты клиента:**

1.1.1. 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.

1.1.2. 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 предоставлять третьим лицам доступ к Устройству, а также к Контактному номеру телефона, не сообщать PIN-код другим лицам, не вводить PIN-код при работе в сети Интернет.

При получении PIN-кода с использованием Сайта для управления услугами или с использованием соответствующего функционала Мобильного приложения Клиенту рекомендуется запомнить PIN-код, полученный в SMS-сообщении от РНКО, после чего удалить полученное от РНКО SMS-сообщение с PIN-кодом и не хранить его на Устройстве и/или SIM-карте во избежание несанкционированного использования такого SMS-сообщения с PIN-кодом третьими лицами.

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

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

1.1.5. 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.

1.1.6. 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, если ему позвонили и назвались представителем какой-либо организации, включая РНКО или Агента, за исключением предоставления Реквизитов Карты клиента микрофинансовой организации в целях погашения задолженности Клиента по договору займа перед данной микрофинансовой организацией.

Перед сообщением Реквизитов Карты Клиент обязан убедиться, что в качестве стороны и (или) представителя стороны, которым Клиент сообщает Реквизиты Карты, выступает такая микрофинансовая организация и (или) ее законный представитель, а такой канал предоставления предусмотрен договором с микрофинансовой организацией.

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.

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

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

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

1.2. Меры безопасности, предпринимаемые Клиентом при использовании Платежного приложения, Платежного кабинета на Интернет-сайте или через Мобильное приложение, а также при совершении операций в сети Интернет с использованием Реквизитов Карты клиента.

1.2.1. Необходимо установить, своевременно обновлять и применять на компьютере и Устройстве в постоянном режиме антивирусные программы. Также рекомендуется регулярно обновлять операционную систему и программы, установленные в ней. Делается это во избежание заражения компьютера, Устройства вирусами и воздействия вредоносных программ, в том числе эксплуатирующих уязвимости программного обеспечения, что может повлечь разглашение третьим лицам Реквизитов Карты клиента, Логина, Пароля, PIN-кода или несанкционированное использование третьими лицами компьютера, Устройства и, как следствие, Платежного приложения, Мобильного приложения или Платежного кабинета.

1.2.2. 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://.

1.2.3. 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.

1.2.4. 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: Visa Secure, Mastercard SecureCode и MirAccept.

1.2.5. 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.

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

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

1.2.8. Необходимо предпринимать меры по сохранности Устройства с установленным Мобильным приложением/ Устройства Apple/ Устройства Samsung/ Устройства Android/ Устройства Mir Pay и не допускать возможности использования Устройства с установленным Мобильным приложением/Устройства Samsung/ Устройства Apple/ Устройства Android/ Устройства Mir Pay третьими лицами, не оставлять Устройство без присмотра.

1.2.9. 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 Платежного приложения Apple Wallet, Google Pay, Samsung Pay, Mir Pay, сверять наименование магазина, указанное в Google Play или AppStore в качестве распространителя программного обеспечения/поставщика Платежного приложения, с наименованием магазина, указанным в настоящих Правилах или в Условиях использования Карты клиента при осуществлении операции с использованием Платежных приложений Apple Wallet, Google Pay, Samsung Pay, Mir Pay.

1.2.10. В случае получения Клиентом предложения об установке любого программного обеспечения, якобы являющегося Мобильным приложением/Платежным приложением Google Pay/ Apple Wallet/ Samsung Pay/ Mir 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.

1.2.11. Клиент должен завершать каждый сеанс работы в Платежном кабинете путем нажатия соответствующей кнопки выхода из Платежного кабинета (сворачивание или закрытие Мобильного приложения в зависимости от технологических настроек может не завершать сеанс работы) 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 Платежным кабинетом, вход в который был ранее осуществлен Клиентом и сеанс работы в котором не завершен, и допускать доступ к ним третьих лиц.

1.2.12. Используя Платежные Приложения Google Pay/Apple Pay/Samsung Pay/Mir 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.

1.2.13. Клиент обязан:

1.2.13.1. обеспечить соответствующий уровень безопасности на своем компьютере и Устройстве, используя пароли, Отпечатки пальцев (Touch ID) или другие возможные методы блокировки/разблокировки Устройства;

1.2.13.2. убедиться, что на Устройстве не зарегистрированы Отпечатки пальцев (Touch ID) или Биометрия лица (Face ID)/Радужка глаза другого лица;

1.2.13.3. не разглашать третьим лицам регистрационные данные от Устройства, такие как Touch ID, пароль. Это конфиденциальная информация;

1.2.13.4. удалить все личные данные и финансовую информацию со старого Устройства, если прекращено его использование;

1.2.13.5. обратиться в Информационный центр по номеру телефона, напечатанному на оборотной стороне Карты клиента либо указанному в Договоре, как можно скорее, в случае подозрений на любое несанкционированное использование Устройства, а также, если Устройство было взломано, потеряно или украдено;

1.2.13.6. не блокировать любые функции безопасности, предусмотренные приложениями Устройства, для использования этих функций и процедур безопасности для защиты всех Карт, зарегистрированных в Мобильном и/или Платежном приложении;

1.2.13.7. создать сложный Пароль при входе в Платежный кабинет (кроме случаев, когда использование Пароля не предусмотрено Договором);

1.2.13.8. удалять информацию о Картах в Платежном приложении/удалять Мобильное приложение при передаче Устройства третьим лицам;

1.2.13.9. не подвергать Устройство операциям повышения привилегий/взлома операционной системы Устройства (root-доступ, разблокировка загрузчика bootloader, Jailbreak и т.п.);

1.2.13.10. незамедлительно изменить Пароль и/или удалить Отпечаток пальца (Touch ID) и/или Биометрию лица (Face ID)/Радужку глаза при возникновении подозрений в их компрометации;

1.2.13.11. самостоятельно осуществлять все операции (действия) в соответствии со своей действительной волей, внимательно изучать информацию, выводимую на экран Устройства, выбирать действия из предлагаемых вариантов в соответствии со своими намерениями, и внимательно проверять правильность вводимой информации.

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

1.3.1. При выявлении операции, содержащей признаки ее осуществления без согласия Клиента, РНКО приостанавливает исполнение соответствующего распоряжения Клиента, а также направляет Клиенту по Контактному номеру 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.

РНКО запрашивает у Клиента подтверждение возобновления исполнения распоряжения путем совершения Клиенту звонка по Контактному номеру телефона с одного из следующих номеров: 8 (383) 335 8088, 8 (383) 335 8811, 8 (383) 230 3870, 8 (383) 286 8603.

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

1.3.2. Одновременно с выполнением действий, предусмотренных п. 1.3.1 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.

1.3.3. 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.

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

1.3.5. При получении от Клиента подтверждения исполнения распоряжения, в том числе путем обращения в Информационный центр, РНКО незамедлительно возобновляет исполнение распоряжения Клиента, при получении от Клиента подтверждения возобновления использования Электронного средства платежа, том числе путем обращения в Информационный центр, РНКО незамедлительно возобновляет использование Клиентом Электронного средства платежа. Указанные действия совершаются РНКО при условии, что Клиент не выполнял действия, предусмотренные п. 1.3.3 настоящих Правил.

1.3.6. 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. 1.3.1 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, понесённые 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/ Платежного приложения Google Pay/ Apple Wallet/ Samsung Pay/ Mir 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 Устройству, в том числе с установленным Мобильным приложением/Платежным Приложением имеет только Клиент; Устройство, в том числе с установленным Мобильным приложением/Платежным приложением не используются третьими лицами. Также Клиент обязуется обеспечивать вышеуказанный режим использования Устройства, в том числе с установленным Мобильным приложением/ /Платежным приложением 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, Устройству, в том числе Устройству, на котором установлено Мобильное приложение/Платежное приложение, Мобильному приложению/Платежному приложению.

2.2.4. Клиент соглашается на передачу распоряжений и/или информации через сеть Интернет, в том числе с использованием Мобильного приложения/Платежного приложения, а также с использованием SMS-сообщения (в случаях, предусмотренных настоящими Правилами), 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 Платежное приложение Клиент принимает на себя риск убытков и иных неблагоприятных последствий, связанный с возможным наличием уязвимостей в Технологии Google Pay/Apple Pay/Samsung Pay/Mir Pay, а также в Платежном приложении. За негативные последствия, связанные с использованием Клиентом Технологии Google Pay/Apple Pay/Samsung Pay/Mir Pay, а также Платежного приложения, 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, Сайтом для управления услугами путем формирования специальных баз данных, признает достоверность сведений в таких базах 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», «Мир».

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

4.1. Получение PIN-кода для соответствующей Карты клиента осуществляется в порядке, предусмотренном Договором.

Отсутствие в Договоре условий о порядке получения PIN-кода для соответствующей Карты клиента означает, что получение PIN-кода не предусмотрено.

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

4.3. 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.

4.4. 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).

4.5. Клиент может получить новый PIN-код в случае утраты/компрометации ранее действовавшего в порядке, предусмотренном Договором.

4.6. Порядок получения нового/измененного PIN-кода в SMS-сообщении с использованием Сайта для управления услугами, если такая возможность дополнительно предусмотрена Договором:

4.6.1. при пополнении Электронного кошелька за счет денежных средств, поступивших в пользу Клиента в РНКО в качестве перевода денежных средств от Займодавца); при замене Карты клиента в порядке, установленном Договором; при обращении Клиента для замены PIN-кода в Информационный центр с использованием Кодового слова:

4.6.1.1. РНКО направляет Клиенту по Контактному номеру телефона SMS-сообщение с уникальной ссылкой, соответствующей определенной Карте клиента, для перехода на Сайт для управления услугами. Клиент обязуется обеспечивать конфиденциальность такого SMS-сообщения и не разглашать его содержание третьим лицам, в том числе, не предоставлять для использования третьим лицам ссылку, Контактный номер телефона (SIM-карту) и Устройство.

4.6.1.2. После перехода на Сайт для управления услугами по ссылке из SMS-сообщения, указанного в п. 4.6.1.1. Правил, Клиент должен подтвердить согласие с порядком получения PIN-кода в SMS-сообщении, отметив соответствующий переключатель (проставив специальную отметку («галочку»)) и нажав кнопку «далее»/«получить». Клиент ознакомлен и согласен с тем, что после подтверждения согласия с условиями о порядке получения PIN-кода, новый/измененный PIN-код будет автоматически сгенерирован и направлен Клиенту в SMS-сообщении по Контактному номеру телефона.

4.6.1.3. После подтверждения Клиентом согласия с порядком получения PIN-кода в SMS-сообщении, РНКО направляет Клиенту по Контактному номеру телефона SMS-сообщение с PIN-кодом для соответствующей Карты клиента.

4.6.2. при самостоятельном переходе на Сайт для управления услугами:

4.6.2.1. Клиент вводит в соответствующие формы Сайта для управления услугами Учетный номер Карты клиента (EAN) и Контактный номер телефона и нажимает кнопку «далее»/ «получить».

4.6.2.2. После ввода данных, Клиент должен подтвердить согласие с условиями получения PIN-кода, отметив соответствующий переключатель (проставив специальную отметку («галочку»)) и нажав кнопку «далее»/«получить», после чего РНКО направляет Клиенту Разовый секретный пароль в SMS-сообщении по Контактному номеру телефона.

4.6.2.3. Для подтверждения волеизъявления Клиента на получение PIN-кода к указанной Карте клиента в SMS-сообщении, требуется ввод Разового секретного пароля, указанного в п. 4.6.2.2 Правил. Клиент ознакомлен и согласен

с тем, что после ввода Разового секретного пароля PIN-код будет направлен ему в SMS-сообщении по Контактному номеру телефона.

4.6.2.4. Если Разовый секретный пароль был введен Клиентом верно, РНКО автоматически генерирует и направляет Клиенту новый/измененный PIN-код в SMS-сообщении по Контактному номеру телефона.

4.6.3. Клиент признает, что совокупность действий, указанных в подпункте 4.6.1.2 настоящих Правил, совершаемая в целях подтверждения волеизъявления Клиента на получение PIN-кода в SMS-сообщении/ввод Разового секретного пароля согласно подпункту 4.6.2.3 настоящих Правил, является аналогом собственноручной подписи, подтверждающим волеизъявление Клиента на получение PIN-кода в SMS-сообщении (при этом ссылка, указанная в п. 4.6.1.2 Правил, является уникальной для соответствующей Карты клиента, позволяет однозначно установить лицо, обратившееся на Сайт для управления услугами с использованием ссылки, в качестве держателя соответствующей Карты клиента).

Указанный способ подтверждения волеизъявления Клиента имеет 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 отправки PIN-кода Клиенту в SMS-сообщении в соответствии с условиями Договора.

4.7. Порядок получения нового/измененного PIN-кода в SMS-сообщении с использованием соответствующего функционала Мобильного приложения, если такая возможность дополнительно предусмотрена Договором:

4.7.1. Клиент нажимает в Мобильном приложении соответствующую кнопку;

4.7.2. РНКО автоматически генерирует и направляет Клиенту новый/измененный PIN-код в SMS-сообщении по Контактному номеру телефона.

4.7.2.1. Клиент может получить новый/измененный PIN-код в SMS-сообщении не более 3 (трех) раз за 1 (один) календарный месяц, за исключением случая, установленного п.4.7.2.2 Правил. В случае исчерпания данного количества SMS-сообщений Клиент может получить новый/измененный PIN-код иным способом, предусмотренным соответствующим Договором.

4.7.2.2. Клиент, использующий Карту клиента типа «KoronaCard», может получить новый PIN-код в SMS-сообщении не более 3 (трех) раз за 1 (один) календарный день и не более 9 (девяти) раз за 1 (один) календарный месяц.

При достижении ограничения, установленного настоящим пунктом Правил для календарного месяца, Клиенту необходимо обратиться в Информационный центр.

4.8. Клиент обязуется обеспечивать конфиденциальность SMS-сообщения с PIN-кодом, полученного по Контактному номеру телефона.

4.9. Клиент выражает свое согласие на получение PIN-кода способами, указанными в разделе 4 настоящих Правил, осознавая, что такой канал передачи информации не всегда является безопасным, и соглашается самостоятельно нести все риски, связанные с возможным нарушением конфиденциальности, возникающие вследствие использования такого канала передачи информации, в том числе связанные с возможным получением информации третьим лицом. В случае несогласия с условиями получения PIN-кода, Клиент обязуется воздержаться от получения PIN-кода указанным способом.

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 (если это предусмотрено условиями Договора):

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 (если это предусмотрено условиями Договора):

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 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 Контактному номеру телефона либо посредством PUSH-уведомления, направляемого на Устройство(-а) с установленным Мобильным приложением «Связной Плюс» (если для оплаты используются Реквизиты Карты клиента типа «Standard», «World» или «World PayPass», на которую нанесен либо логотип «Кукуруза», либо логотип «Связной Плюс») или на Устройство(-а) с установленным Мобильным приложением «Карта Билайн» (если для оплаты используются Реквизиты Карты клиента типа «Билайн», «Билайн World», «Билайн World PayPass» или «Beeline Gaming») или на Устройство (-а) с установленным Мобильным приложением «Ozon.Card» (если для оплаты используются Реквизиты Карты клиента «o.mycard»), после запроса Клиента на предоставление Разового секретного пароля (технология Mastercard Secure Code, или Visa Secure, или MirAccept). 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. Если ввод Разового секретного пароля не запрошен, то направление Клиентом РНКО электронного документа (в т.ч. ЭПД) подтверждается нажатием предлагаемой экранной формой кнопки (например, «оплатить», «подтвердить», «подписать» и т.д.), в результате чего электронному документу (в т.ч. ЭПД) присваивается уникальный набор символов, сформированный для Клиента при нажатии кнопки.

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

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.

9. Доступ к СЕРВИСУ, работа в СЕРВИСЕ

9.1. Доступ Клиента к Сервису осуществляется после успешного прохождения Клиентом процедуры Идентификации, если возможность использования Сервиса предусмотрена Договором. РНКО вправе по собственному усмотрению потребовать, чтобы Клиент подтвердил свое волеизъявление осуществить вход в Платежный кабинет (если Идентификация Клиента осуществлялась с использованием Логина и Пароля). Для этого Клиенту необходимо ввести Разовый секретный пароль, направленный РНКО Клиенту по Контактному номеру телефона в виде SMS-сообщения либо по усмотрению РНКО и при наличии технической возможности PUSH-уведомлением.

9.2. РНКО и Клиент признают, что Логин и Пароль/Разовый секретный пароль, используемые Клиентом при прохождении процедуры Идентификации, являются уникальными.

9.3. Первый вход в Платежный кабинет осуществляется с использованием EAN в качестве Логина (за исключением случая, предусмотренного п.9.3.1 настоящих Правил). После ввода Логина Клиент вводит Разовый секретный пароль, направленный РНКО Клиенту в виде SMS-сообщения по Контактному номеру телефона. Пароль устанавливается Клиентом самостоятельно при первом входе в Платежный кабинет.

9.3.1. Первый и последующий входы в Платежный кабинет Клиента, использующего Карту клиента типа «KoronaCard», осуществляются с использованием Контактного номера телефона в качестве Логина. После ввода Логина Клиент вводит Разовый секретный пароль, направленный РНКО Клиенту по Контактному номеру телефона в виде SMS-сообщения либо по усмотрению РНКО и при наличии технической возможности PUSH-уведомлением. Установка Пароля для Клиента, использующего Карту клиента типа «KoronaCard», не предусмотрена. При входе в Платежный кабинет Логин сохраняется автоматически и на экране Устройства (используемого Клиентом для входа в Платежный кабинет) может не отображаться.

9.4. Использование Контактного номера телефона в качестве Логина:

9.4.1. Клиенту, использующему Карту клиента типа «KoronaCard», предоставляется возможность использования в качестве Логина только Контактного номера телефона.

9.4.2. Клиенту, использующему Карту клиента типа «Билайн», «Билайн World», «Билайн World PayPass» или «Beeline Gaming» или Карту клиента типа «Standard», «World», «World PayPass» (на которую нанесен либо логотип «Кукуруза», либо логотип «Связной Плюс») или Карту клиента «o.mycard», после осуществления Клиентом первого входа в Платежный кабинет через соответствующий типу Карты клиента интернет-сайт или Мобильное приложение, предоставляется возможность использования в качестве Логина Контактного номера телефона.

Исключение составляют случаи, когда возможность входа по Контактному номеру телефона уже предоставлена Клиенту, в том числе с использованием другого Логина, либо Клиент запретил использование в качестве Логина Контактный номер телефона.

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

9.4.3. В случае изменения Контактного номера телефона, используемого в качестве Логина для входа в Платежный кабинет, Логин Клиента будет соответствовать измененному Контактному номеру телефона, при этом замена ранее установленного Клиентом Пароля (если установка Пароля предусмотрена Договором или настоящими Правилами) не требуется.

9.4.4. Если установка Пароля предусмотрена Договором или настоящими Правилами, для доступа к Платежному кабинету Клиент применяет один Пароль при использовании в качестве Логина как EAN Карты Клиента, так и Контактного номера телефона.

9.4.5. 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 Контактный номер телефона.

9.5. Особенности входа в Платежный кабинет через Мобильное приложение (если использование Пароля предусмотрено Договором или настоящими Правилами):

9.5.1. Мобильное приложение предоставляет Клиенту возможность пройти Идентификацию с использованием Пароля, состоящего из 4 (четырех) 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 инсталлированного на конкретное устройство Клиента Мобильного приложения. При этом в качестве Логина в таком случае используется совокупность EAN или Контактного номера

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.

9.5.2. 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», «Билайн World», «Билайн World PayPass», «Beeline Gaming» (для Устройств с iOS или Android); или «Standard», «World», «World PayPass», на которую нанесен либо логотип «Кукуруза», либо логотип «Связной Плюс» (для Устройств с iOS или Android); или «o.mycard».

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 9.8 настоящих Правил) возлагаются на Клиента.

9.6. 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 Контактному номеру 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.

9.7. 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 Контактный номер 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.

9.8. 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. 9.7 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;

9.9. Доступ Клиента в Платежный кабинет может быть временно заблокирован без предварительного уведомления Клиента после трёхкратного последовательного ввода Клиентом неправильного Пароля (если использование Пароля предусмотрено Договором или настоящими Правилами). В данном случае происходит блокировка Логина на 180 (Сто восемьдесят) секунд. После трех последовательных блокировок Логина обслуживание Клиента в Сервисе приостанавливается. 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 Контактному номеру телефона.

9.10. Доступ в Платежный кабинет Клиента, использующего Карту клиента типа «KoronaCard», может быть временно заблокирован без предварительного уведомления Клиента после десятикратного ввода Клиентом неправильного Разового секретного пароля. В данном случае происходит блокировка Логина на 300 (Триста) секунд.

9.11. 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.

9.12. 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.

9.13. 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.

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

9.15. 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.

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

9.17. 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.

9.18. 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 Контактному номеру телефона.

9.19. Держатели Карт клиента типа «Standard», «World», «World PayPass» (на которые нанесен либо логотип «Кукуруза», либо логотип «Связной Плюс»), держатели Карт клиента типа «Билайн», «Билайн World», «Билайн World PayPass», «Beeline Gaming», 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.plus.svyaznoy.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 «Связной Плюс» 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 Контактный номер телефона. Для Платежного кабинета, доступ к которому осуществляется через сайт oplata.plus.svyaznoy.ru, bank.beeline.ru oplata.kari.com, pay.khclub.ru,

pay.domadengi.ru, pay.otlnal.ru или pay.mycard.ru, либо через Мобильное приложение «Связной Плюс» или «Карта Билайн», подключение осуществляется автоматически при первом входе в Платежный кабинет.

Мобильные приложения «Связной Плюс» 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).

9.20. Управление Электронным кошельком недоступно Клиенту, если он направил РНКО уведомление для блокировки соответствующего Электронного средства платежа в порядке, предусмотренном Договором, в связи с его утратой или компрометацией, а также если такое Электронное средство платежа блокировано по инициативе РНКО в предусмотренных Договором случаях.

При наличии у Клиента нескольких Электронных средств платежа (используемых Клиентом в рамках одного Договора), хотя бы одно из которых не было заблокировано, Клиент осуществляет вход в Платежный кабинет с использованием в качестве Логина Контактного номера телефона или EAN Карты клиента, соответствующих незаблокированному Электронному средству платежа.

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.

9.21. В случае блокировки Электронных средств платежа, используемых в рамках одного Договора, по инициативе Клиента, возможность доступа в Платежный кабинет для Клиента сохраняется с целью подачи заявлений в РНКО, просмотра информации, без права распоряжения электронными денежными средствами.

В случае блокировки Электронных средств платежа, используемых в рамках одного Договора, по инициативе РНКО, в связи с подозрением на неправомерное использование Электронных средств платежа злоумышленниками, без согласия Клиента, возможность входа в Платежный кабинет полностью блокируется. В остальных случаях блокировки Электронных средств платежа, используемых в рамках одного Договора, по инициативе РНКО, возможность входа в Платежный кабинет сохраняется с целью подачи заявлений в РНКО, просмотра информации, без права распоряжения электронными денежными средствами.

9.21.1. В случае блокировки Электронного средства платежа, используемого в рамках Договора и соответствующего Карте клиента типа «KoronaCard», по инициативе Клиента либо по инициативе РНКО, возможность доступа в Платежный кабинет сохраняется без права распоряжения электронными денежными средствами.

9.22. Валютные электронные кошельки могут быть созданы по запросу Клиента в Платежном кабинете, доступ к которому осуществляется с сайтов oplata.plus.svyaznoy.ru, bank.beeline.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 Логином.

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

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.

10.1.4. 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. 9.18 Правил либо установленные в Договоре.

• отсутствует или технически прекращена возможность переводов через Платежный кабинет в пользу определенного Получателя

• иных случаях, предусмотренных Договором.

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) 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).

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 о переводе ЭДС или Распоряжения возврате Остатка ЭДС.

11. Уведомления

11.1. 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 Контактному номеру телефона или направления PUSH-уведомлений в Мобильном приложении в порядке, предусмотренном Договором.

Предоставление Клиенту Разового секретного пароля осуществляется РНКО посредством направления SMS-сообщений по Контактному номеру 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.

11.2. **Подключение информирования PUSH-уведомлениями:**

11.2.1. На устройство с установленным Мобильным приложением «Связной Плюс» (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.

11.2.2. На устройство с установленным Мобильным приложением «Связной Плюс» (версия приложения для Android – 2.5 и выше, версия приложения для iOS – 2.0 и выше), или 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:

11.2.2.1. 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.

11.2.2.2. PUSH-уведомлениями с целью получения Разовых секретных паролей, подтверждается Клиентом:

11.2.2.2.1. Если Клиент до «30» мая 2022 года уже совершил успешный вход в Платежный кабинет с использованием Мобильного приложения, путем ввода Разового секретного пароля, направляемого посредством SMS-сообщения по Контактному номеру 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.

11.2.2.2.2. Если Клиент совершает вход в Платежный кабинет с использованием Мобильного приложения после «30» мая 2022 года, путем ввода Разового секретного пароля, направляемого посредством SMS-сообщения по Контактному номеру телефона при осуществлении Клиентом первого входа в Платежный кабинет через соответствующее типу Карты клиента Мобильное приложение.

Изменение способа получения уведомлений с Разовыми секретными паролями не предусмотрено.

11.2.3. На устройстве с установленным Мобильным приложением «Денежные переводы» подключение информирования PUSH-уведомлениями с целью получения Информационных уведомлений не предусмотрено.

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

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

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

11.6. 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.

11.7. 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.

11.8. 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.

ПРИЛОЖЕНИЕ №1
к Правилам использования Карты клиента и работы в Сервисе «Интернет Платежи»

Условия использования Карты клиента при осуществлении операции с использованием Платежных приложений Apple Wallet, Google Pay, Samsung Pay, Mir Pay

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Платежное приложение (Приложение) – программное обеспечение, предоставляемое Поставщиком платежного приложения, установленное на Устройстве и предназначенное для совершения Клиентом переводов денежных средств, в том числе в Платежном кабинете, при помощи беспроводной связи без физического использования Карты по технологии NFC («ближняя бесконтактная связь») или Samsung MST (Magnetic Secure Transmission), 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 Платежном приложении может не соответствовать реальному дизайну Карты клиента. Платежное приложение может быть предустановлено на Устройстве либо Клиент вправе самостоятельно установить Платежное приложение в программе-магазине для поиска и загрузки приложений на Устройстве (Google Play). Перечень Платежных приложений, Поставщиков Платежных приложений, типов Карты клиента, для которой возможно использование Платежного приложения, приведен в Таблице №1 ниже по тексту.

Таблица №1

Наименование Платежного приложения	Поставщик Платежного приложения	Наименование магазина	Тип Карты клиента, для которой возможно использование Платежного приложения
Платежное приложение Apple Wallet, работающее по технологии Apple Pay. **Apple Pay** – технология мобильных платежей, позволяющая Клиенту совершать операции с ЭДС при помощи Устройства с операционной системой iOS.	«ЭППЛ ДИСТРИБЬЮШН ИНТЕРНЭШНЛ» (APPLE DISTRIBUTION INTERNATIONAL) - ирландская корпорация с неограниченной ответственностью, с местонахождением основного коммерческого предприятия по адресу: Промышленная зона Холли Хилл, Корк, Ирландия (Holly Hill Industrial Estate, Cork, Ireland)	Нет. **Платежное приложение Apple Wallet** предустановлено на устройство	Возможность использования Платежного приложения не предоставляется по независящим от РНКО причинам.
Платежное приложение Google Pay, работающее по технологии Google Pay. **Google Pay** – технология мобильных платежей, позволяющая Клиенту совершать операции с ЭДС при помощи Устройства с операционной системой Android.	Google Ireland Limited; Гордон Хаус, Бэрроу Стрит, Дублин 4, Ирландия (Gordon House, Barrow Street, Dublin 4, Ireland)	**Google LLC**	Возможность использования Платежного приложения не предоставляется по независящим от РНКО причинам.
Платежное приложение Samsung Pay, работающее по	Самсунг Электроникс Ко., Лтд. Маетан-донг, 129, Самсунг-Ро,	**Samsung Electronics Co., Ltd.**	Карты клиента «Билайн» / «Билайн World» / «Билайн World PayPass» / «Beeline Gaming»;

технологии Samsung Pay. **Samsung Pay** – технология мобильных платежей, позволяющая Клиенту совершать операции с ЭДС при помощи Устройства от производителя Samsung с операционной системой Android или Tizen.	Йонгтонг-гу, Сувон-си, Гиёнги-до / Samsung Electronics Co., Ltd Maetan-dong, 129, Samsung-ro, Youngtong-gu, Suwon-si, Gyeonggi-do		Карты клиента «Standard» / «World» / «World PayPass» (на которые нанесен либо логотип «Кукуруза», либо логотип «Связной Плюс»); Карты o.mycard 300, Карты o.mycard 60; Карты «KoronaCard» платежной системы «Мир»; 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). Доступно добавление и использование карт платежной системы «Мир». В настоящее время по независящим от РНКО причинам могут быть недоступны некоторые операции: - Добавление карт Mastercard; - Оплата с помощью Samsung Pay картами Mastercard
Платежное Приложение Mir Pay, работающее по технологии Mir Pay **Mir Pay -** технология мобильных платежей, позволяющая Клиенту совершать операции с ЭДС в ЭК, соответствующем Карте, принадлежащей к платежной системе «Мир», при помощи Устройства с операционной системой Android.	Акционерное общество «Национальная система платежных карт», ОГРН 1147746831352, Российская Федерация, 115184, город Москва, улица Большая Татарская, дом 11.	**Google LLC** **Huawei Services (Hong Kong) Co., Limited**	Карты «KoronaCard» платежной системы «Мир»; Карты клиента платежной системы «Мир», перечисленные на сайте rnko.ru в разделе «Карты – Виртуальная подарочная» (доступном по адресу http://rnko.ru/individualcards/Pages/default.aspx); Карты клиента платежной системы «Мир», перечисленные на сайте rnko.ru в разделе «Карты – Виртуальная карта питания» (доступном по адресу http://rnko.ru/individualcards/Pages/default.aspx).

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

Токенизация – процесс создания Токена (DPAN) и его связки с PAN Карты клиента, позволяющий однозначно определить Карту клиента, использованную для совершения операций с использованием Платежного приложения. Токенизация осуществляется по факту добавления Карты в Платежное приложение.

Touch ID (Отпечаток пальца) – однозначное цифровое представление рисунка кожи на пальце руки Клиента, зафиксированное дактилоскопическим датчиком/сканером отпечатков пальцев, предустановленным в Устройстве Клиента. Отпечаток пальца обеспечивает однозначное определение Клиента. Отпечаток пальца при совершении Клиентом операции с использованием Карты посредством Платежного приложения признается простой электронной подписью Клиента и может использоваться многократно.

Face ID (Биометрия лица)/Радужка глаза – однозначное цифровое представление лица или радужки глаза Клиента, зафиксированное биометрическим сканером распознавания формы лица или радужки глаза, предустановленным в Устройстве Клиента. Подтверждение с использованием Биометрии лица или Радужки глаза при совершении Клиентом операции с использованием Карты посредством Платежного приложения признается аналогом собственноручной подписи Клиента и может использоваться многократно.

POS-терминал — электронное программно-техническое устройство для приёма к оплате банковских платежных карт. Оно может принимать карты с чипом, магнитной полосой и бесконтактные карты, а также другие устройства, имеющие бесконтактное сопряжение. Также под POS-терминалом подразумевается весь программно-аппаратный комплекс, который установлен на рабочем месте кассира.

Термины, не определенные в настоящих Условиях использования Карты клиента при осуществлении операции с использованием Платежных приложений Apple Wallet, Google Pay, Samsung Pay, Mir Pay (далее – Условия), применяются в том значении, в котором они определены в Договоре о комплексном обслуживании клиента (далее – Договор) или Правилах использования Карты клиента и работы в Сервисе «Интернет Платежи». Во всех иных случаях такие термины

применяются в том значении, в каком они используются в соответствующей отрасли законодательства Российской Федерации.

2. Общие положения

2.1. Настоящие Условия являются неотъемлемой частью Договора. Все, что не определено настоящими Условиями, определено Договором, Правилами использования Карты клиента и работы в Сервисе «Интернет Платежи», Перечнем ограничений по операциям, Специальными условиями обслуживания при оказании Услуги «SMS-уведомления», Правилами перевода денежных средств с указанием номера мобильного телефона, Правилами транслитерации при совершении переводов денежных средств без открытия счета «Золотая Корона», и обязательно для исполнения РНКО и Клиентом.

Клиент присоединяется к настоящим Условиям использования Карты клиента при осуществлении операции с использованием Платежных приложений Apple Wallet, Google Pay, Samsung Pay, Mir Pay (далее Условия) в соответствии со ст.428 Гражданского кодекса Российской Федерации в момент регистрации Клиентом Карты клиента в Платежном приложении. При этом фиксация присоединения Клиента к настоящим Условиям осуществляется РНКО в электронном виде в программном обеспечении РНКО в момент регистрации Карты клиента в Платежном приложении.

Регистрация Карты клиента в Платежном приложении означает, что Клиент ознакомлен и согласен с настоящими Условиями.

РНКО не является владельцем (разработчиком) Платежного приложения и не осуществляет поддержку программного обеспечения Платежного приложения.

РНКО не взимает комиссию за использование Карты клиента посредством Платежного приложения.

Настоящие Условия действуют до расторжения (прекращения) Договора, или до удаления Клиентом Платежного приложения с Устройства либо последнего Токена Карты клиента из Платежных приложений, или до прекращения РНКО договорных отношений с Поставщиком Платежного приложения. Прекращение действия настоящих Условий и/или Договора не влияет на юридическую силу и действительность распоряжений, направленных Клиентом до прекращения действия Условий и/или Договора.

Использование технологии Apple Pay, Google Pay, Samsung Pay, Mir Pay в POS-терминалах возможно только в случае онлайн Авторизации платежей.

Принимая настоящие Условия, Клиент дает согласие на получение sms-сообщений/PUSH-уведомлений на Устройство.

Принимая настоящие Условия, Клиент понимает и согласен с тем, что:

2.1.1. доступ, использование и возможность совершения платежей посредством реквизитов Карты в Платежном приложении зависит от Поставщика платежного приложения, от состояния сетей беспроводной связи;

2.1.2. РНКО не контролирует и не влияет на обслуживание беспроводных сетей связи, на систему отключения/прерывания беспроводного соединения.

2.1.3. РНКО не гарантирует конфиденциальность и безопасность передачи данных в связи с электронной передачей данных через сторонние подключения, не попадающие под контроль РНКО. Обеспечение конфиденциальности и безопасности передачи данных осуществляется в соответствии с регламентами Поставщика платежного приложения.

2.1.4. РНКО не несет ответственности за поддержку операционной системы Устройства.

3. Регистрация Карты клиента в Платежном приложении

3.1. Для совершения операций с использованием Карты клиента, типы которых перечислены в Таблице №1, посредством Платежного приложения Apple Wallet, или Google Pay, или Samsung Pay, или Mir Pay Клиенту необходимо зарегистрировать Карту клиента в соответствующем Платежном приложении.

Регистрация Карты клиента в соответствующем Платежном приложении осуществляется в соответствии с инструкциями Платежных приложений, одним или несколькими из следующих способов:

- автоматическое заполнение реквизитов Карты клиента в Платежном приложении с использованием камеры Устройства;

- путем ввода реквизитов Карты клиента в Платежном приложении вручную;

- используя иной способ, определяемый Поставщиком (при наличии технической возможности).

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.

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.

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/.

Подробная информация о Mir Pay и Устройствах Mir Pay, а также инструкции по использованию Mir Pay доступны на сайте https://mironline.ru/mirpay/

Зарегистрировать Карту клиента в Apple Wallet/ Google Pay/ Mir Pay при наличии технической возможности возможно также в Мобильном приложении, выполняя действия, информация о которых отображается на экране Устройства в разделе Мобильного приложения «Добавить в Google Pay»/ «Добавить в Apple Pay/ «Добавить в Mir Pay» (наименование раздела Мобильного приложения может отличаться от указанного в настоящих Условиях, но аналогично по смыслу).

Если у Клиента возникли какие-либо проблемы с регистрацией Карты клиента в Apple Wallet/ Google Pay/ Samsung Pay/ Mir Pay Клиенту необходимо обратиться в Информационный центр.

3.2. РНКО осуществляет регистрацию Карты клиента после ввода Клиентом Разового секретного пароля, полученного в PUSH-уведомлении или sms-сообщении по Контактному номеру телефона. Действительность направленного РНКО пароля составляет от 5 (Пяти) до 10 (Десяти) минут.

3.3. Клиент выражает согласие (акцепт) с текстом настоящих Условий путем проставления отметки о принятии Условий в соответствующем поле в экранной форме Платежного приложения.

3.4. По факту успешно проведенной регистрации Карты клиента в Платежном приложении формируется Токен. Реквизиты Карты клиента заменяются на цифровой код – созданный Токен. Токен позволяет однозначно идентифицировать Карту клиента, используемую при совершении операций с использованием Карты клиента посредством Платежного приложения.

3.5. Клиенту поступает sms-сообщение/PUSH-уведомление об успешной регистрации Карты клиента в Платежном приложении незамедлительно после регистрации Карты клиента в Платежном приложении.

3.6. Ограничения по количеству Устройств, на которые можно зарегистрировать одну Карту клиента в Платежном приложении и по количеству банковских карт, которые можно зарегистрировать на одном Платежном приложении, устанавливаются Поставщиком платежного приложения и/или Платежной системой.

3.7. Клиент может самостоятельно удалить один или несколько Токенов из Платежного приложения, следуя инструкциям в Платежном приложении.

4. Порядок совершения и подтверждения операции

4.1. Операции с использованием Карты клиента посредством Платежного приложения могут осуществляться:

4.1.1. через POS-терминал, оснащенный NFC, – для Платежного приложения Apple Wallet, Google Pay, Samsung Pay, Mir Pay; или через POS-терминал, предназначенный для считывания банковских карт с магнитной полосой (не оснащенный NFC), – для Платежного приложения Samsung Pay;

4.1.2. в мобильных приложениях на Устройстве и на сайтах интернет-магазинов, поддерживающих оплату покупок посредством Платежного приложения (где доступна кнопка «Оплатить Apple Pay», или «Оплатить Google Pay», или «Оплатить Samsung Pay»), поддерживающих расчеты через Платежные приложения.

4.1.3. в устройствах самообслуживания (банкоматах, информационно-платежных терминалах), оснащенных NFC, – для Платежного приложения Apple Wallet, Google Pay, Samsung Pay.

Более подробная информация о способах оплаты доступна:

для Технологии Samsung Pay на сайте http://www.samsung.com/ru/apps/mobile/samsungpay/;

для Технологии Apple Pay - https://support.apple.com/ru-ru/HT201239;

для Технологии Google Pay - https://support.google.com/pay/answer/6224811?hl=ru.

4.2. Совершение операций с использованием Карты клиента посредством Платежного приложения возможно во всех позволяющих совершать операции посредством Платежного приложения устройствах самообслуживания, ТСП Mastercard, ТСП Visa или ТСП «Мир».

4.3. Подтверждение операции с использованием Технологии Apple Pay/ Google Pay/ Mir Pay может осуществляться путем ввода Клиентом пароля для разблокировки Устройства (что признается подтверждением распоряжения клиента аналогом собственноручной подписи), или с помощью Touch ID (Отпечаток пальца), или с помощью Face ID (Биометрия лица) (если Устройство поддерживает технологию распознавания Отпечатка пальца или технологию Биометрии лица).

Подтверждение операции с использованием Технологии Samsung Pay может осуществляться после разблокировки Устройства путем ввода Клиентом пароля для разблокировки Платежного приложения (что признается подтверждением распоряжения клиента аналогом собственноручной подписи), или с помощью Touch ID (Отпечаток пальца), или с помощью Радужки глаза (если Устройство поддерживает технологию распознавания Отпечатка пальца или технологию распознавания Радужки глаза).

4.4. При наличии двух и более банковских платежных карт, в том числе карт других банков-эмитентов, зарегистрированных в Платежном приложении, Клиент выбирает Карту клиента, с использованием которой будут осуществляться операции посредством Платежного приложения.

4.5. По завершении платежной операции в POS-терминале кассир должен выдать Клиенту чек. По завершении операции в устройстве самообслуживания рекомендуется получить чек, проверить информацию, содержащуюся в чеке.

В чеке при совершении операции с использованием Платежного приложения помимо прочей информации указываются последние 4 цифры Токена, хранящегося в Устройстве, с помощью которого произведена оплата.

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

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

4.7.1. Для Технологии Samsung Pay 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/);

4.7.2. Для Технологии Apple Pay приостановить или полностью запретить оплату покупок через Apple Pay для iPhone или iPad на странице учетной записи Apple ID или в программе «Найти iPhone» (https://apps.apple.com/ru/app/find-my-iphone/id376101648).

4.7.3. Для Технологии Google Pay/Mir Pay воспользоваться функцией «Найти устройство», либо скачать приложение «Найти устройство» в Google Play (https://support.google.com/accounts/answer/6160491).

В данном случае РНКО блокирует только Токен, содержащийся на данном Устройстве.

4.8. С целью дополнительного обеспечения безопасности использования Платежных приложений, Поставщик платежного приложения вправе устанавливать дополнительные условия использования Платежного приложения, совершения платежей, информация о которых доводится до Клиента в Мобильном приложении/информационными сообщениями Поставщика платежного приложения.

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

4.9. Используя Платежное приложение, Клиент дает РНКО поручение направлять Поставщику платежного приложения информацию об операциях, совершаемых Клиентом с использованием Платежного приложения (в том числе, дату и время операции, сумму операции, валюту операции, наименование и/или адрес ТСП, статус сделки, код категории отрасли, название категории отрасли, код отрасли и название отрасли).

Упомянутая в настоящем пункте информация об операциях направляется с целью предоставления Поставщику платежного приложения и его аффилированным лицам возможности использовать такую информацию, в частности, для:

- предоставления Клиенту истории операций такого Клиента, совершенных с использованием Платежного приложения;
- обнаружения и устранения мошенничества;
- создания отчетов об экономической эффективности Платежного приложения исключительно для использования внутри компании Поставщика;
- усовершенствования Платежного приложения;
- рекламы Платежного приложения и проведения анализа распределения рекламных объявлений.

4.10. В случае использования Платежного приложения Клиент соглашается с тем, что РНКО может получать от Поставщика платежного приложения данные Устройства (в том числе марку/модель Устройства, IMEI Устройства и иные данные Устройства) в целях использования таких данных для технической поддержки Клиентов, разрешения споров, обнаружения и устранения мошенничества.

4.11. Поставщик платежного приложения имеет право по своему усмотрению приостановить или прекратить предоставление Клиенту возможности осуществления оплат с применением Платежного приложения.

5. Меры безопасности

5.1. В целях минимизации риска хищения денежных средств и обеспечения совершения операций с использованием банковских карт посредством Платежного приложения Клиент обязан обеспечить выполнение требований, установленных разделом 1 Правил использования Карты клиента и работы в Сервисе «Интернет Платежи».

6. Права и обязанности сторон

6.1. РНКО вправе:

6.1.1. Отказать в регистрации Карты клиента в Платежном приложении с учетом недостаточного Остатка ЭДС на Карте клиента либо в связи с низкой оценкой безопасности использования Устройства, полученной от Поставщика Платежного приложения.

6.1.2. Отказать Клиенту в совершении операции по зарегистрированной Карте клиента в Платежном приложении:

6.1.2.1. если операция противоречит требованиям действующего законодательства Российской Федерации, Договору, Правилам использования Карты клиента и работы в Сервисе «Интернет Платежи», настоящим Условиям или порядку осуществления данной операции, установленному платежной системой и/или действующим законодательством Российской Федерации;

6.1.2.2. если Клиентом не соблюдены требования действующего законодательства Российской Федерации, настоящих Условий;

6.1.2.3. если у РНКО возникли подозрения в том, что операция инициирована не Клиентом;

6.1.2.4. если у РНКО возникли подозрения, что операция осуществляется в целях легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма;

6.1.2.5. если Клиентом в случаях и в сроки, предусмотренные действующим законодательством Российской Федерации, Договором, не предоставлены документы и сведения, необходимые для идентификации физических лиц, и/или раскрывающие экономический смысл и подтверждающие законный характер операций;

6.1.2.6. в иных случаях, предусмотренных Договором, Условиями, действующим законодательством Российской Федерации.

6.1.3. Ограничить, приостановить или прекратить использование Карты клиента в Платежном приложении в случаях, указанных в п.6.1.2. настоящих Условий.

6.1.4. По своему усмотрению устанавливать лимиты на суммы и по количеству операций при совершении операции с использованием Карты клиента посредством Платежного приложения. Лимиты установлены Перечнем ограничений по операциям.

6.1.5. В одностороннем порядке изменять настоящие Условия в порядке, предусмотренном Договором.

6.1.6. В установленных законодательством Российской Федерации случаях осуществлять в отношении Клиента контрольные и иные функции, возложенные на РНКО законодательством Российской Федерации, в связи с чем

запрашивать у Клиента любые необходимые документы и (или) письменные пояснения относительно характера и экономического смысла предполагаемых или совершенных операций с использованием Реквизитов Карты в Платежном приложении.

6.2. РНКО обязуется:

6.2.1. Исполнять распоряжения Клиента, направленные с использованием Платежного приложения, в порядке и на условиях, установленных Договором;

6.2.2. Заблокировать Токен(-ы) на Устройстве после получения соответствующего обращения Клиента.

6.2.3. Информировать Клиента о каждой операции, совершенной с использованием Карты клиента посредством Платежного приложения в порядке и способами, предусмотренными Договором.

6.3. Клиент вправе:

6.3.1. Приостановить действие Токена/удалить Токен, обратившись в РНКО лично или через Информационный центр, или с помощью функции в Платежном приложении.

6.3.2. Обращаться в РНКО с заявлениями, в том числе при возникновении споров, связанных с операциями, совершенными с использованием Карты клиента посредством Платежного приложения, а также получать информацию о результатах рассмотрения заявлений в порядке, определенном Договором.

6.4. Клиент обязуется:

6.4.1. Соблюдать настоящие Условия, Договор, Правила использования Карты клиента и работы в Сервисе «Интернет Платежи», и условия договоров с третьими лицами (договоры с Поставщиком платежного приложения, оператором мобильной связи и другими сторонними поставщиками услуг, которые включены в систему платежных услуг).

6.4.2. Соблюдать меры безопасности при использовании Платежного приложения.

6.4.3. Обеспечить конфиденциальность, а также хранение Устройства, Пароля, SIM-карты способом, исключающим доступ к ним третьих лиц, а также немедленно уведомлять РНКО о подозрении, что Устройство, Пароль, SIM-карта – могут быть использованы посторонними лицами.

В случае утраты Клиентом Устройства, Пароля, SIM-карты или наличия подозрений, что они используются третьими лицами, Клиент должен незамедлительно, после обнаружения указанных фактов, но не позднее дня, следующего за днем получения от РНКО уведомления о совершенной операции, сообщить об этом РНКО.

На основании сообщения, РНКО блокирует Токен. Отсутствие предусмотренного настоящим пунктом сообщения со стороны Клиента лишает Клиента права на получение возмещения от РНКО по операциям, совершенным без согласия Клиента.

6.4.4. Оказывать содействие РНКО при проведении расследований в случае несанкционированного списания денежных средств, предоставлять РНКО необходимые документы и информацию.

7. Ответственность сторон

7.1. Клиент несет ответственность перед РНКО в соответствии с требованиями действующего законодательства Российской Федерации, в том числе за убытки, возникшие у РНКО в результате совершения операции с использованием Карты клиента посредством Платежного приложения от имени Клиента неуполномоченным лицом с использованием принадлежащего Клиенту Устройства, Пароля, Отпечатка пальца, Биометрии лица и иной конфиденциальной информации.

7.2. Доступ, использование и обслуживание Токена зависят от Поставщика платежного приложения и сети оператора мобильной связи. РНКО не является Поставщиком платежного приложения или указанной сети и не контролирует их действия. РНКО не несет ответственность перед Клиентом за любые обстоятельства, которые могут прервать, создать препятствия или иным образом отразиться на функционировании любого Токена, включая недоступность услуг Платежного приложения или услуг беспроводной связи, коммуникаций, задержек сети, ограничений беспроводного покрытия, сбоев системы или прерывание беспроводной связи.

7.3. РНКО не несет ответственности за безопасность, точность, законность, пригодность и другие аспекты содержания или функционирования продуктов или услуг Поставщика платежного приложения.

7.4. РНКО не несет ответственности, а также не предоставляет клиентскую поддержку в отношении любого аппаратного или программного обеспечения третьей стороны, а также ее иных продуктов или услуг (включая Платежное приложение или Устройство). В случае возникновения любых вопросов в связи с использованием продуктов или услуг третьей стороны, Клиент должен обращаться непосредственно к третьей стороне для получения клиентской поддержки.

Председатель Правления ***подпись*** **Г.М. Мац**

«15» июля 2022 года