Приложение №3

к Приказу №670/1 от 17.11.2020 г.

Изменения в ПРАВИЛА
дистанционного банковского обслуживания физических лиц
в Системе «iBank2» в ООО КБ «РостФинанс»

г. Ростов-на-Дону
2020 год

Настоящие изменения в Правила дистанционного банковского обслуживания физического лица в Системе ДБО «iBank2» в ООО КБ «РостФинанс» (далее по тексту именуемые – «Правила дистанционного банковского обслуживания физического лица» / «Правила») приняты в соответствии с пунктами 14.2 - 14.4. Правил дистанционного банковского обслуживания физического лица, утвержденных Протоколом Правления ООО КБ «РостФинанс» №68 от 31.08.2020г.

Настоящие изменения в Правила вступают в силу «02» декабря 2020г. (размещены на информационных стендах в подразделениях Банка и на сайте Банка www.rostfinance.ru в сети Интернет «17» ноября 2020г.).

Стороны приняли решение изменить в Правилах дистанционного банковского обслуживания физического лица и всех сопутствующих документах, утвержденных Протоколом Правления ООО КБ «РостФинанс» №68 от 31.08.2020г., наименование «Система «iBank2» на «Система «ДБО».

Стороны приняли решение изложить Правила дистанционного банковского обслуживания физического лица в новой нижеуказанной редакции.

Содержание

1.Основные понятия и сокращения

Аутентификация клиента (Аутентификация) – положительный результат процедуры проверки и подтверждения Пароля и/или Одноразового пароля, применяемого Банком и Клиентом для организации и/или проведения Операций, получения информации по Счету в Системе ДБО, совершения других действий в рамках Договора в порядке, предусмотренном в настоящих Правилах. Для проведения Аутентификации Клиент должен использовать уникальные аутентификационные данные (совокупность данных).

ПЭП – простая электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования Электронной подписи определенным лицом. Применяется в Системе ДБО как средство проверки авторства электронных документов.

Банк – Общество с ограниченной ответственностью коммерческий банк «РостФинанс» (ООО КБ «РостФинанс») и его структурные подразделения.

Банковская карта (Карта) – расчетная платежная карта, являющаяся персонализированным банковским средством, предназначенным для оплаты товаров, услуг и получения наличных денег в пределах расходного лимита, является собственностью Банка и выпускается к Счету карты.

Банковский счет (Счет) – счет Клиента, открытый в Банке для осуществления Операций в порядке и на условиях, предусмотренных соответствующим договором текущего счета/договором вклада/договором текущего счета с использованием банковской карты, на основании которого открыт банковский счет.

Временный пароль – Пароль, который выдается и направляется Банком Клиенту при регистрации Клиента в Системе ДБО, действующий ограниченное время до момента самостоятельного создания Клиентом постоянного Пароля при первом входе в Систему ДБО.

ДБО – дистанционное банковское обслуживание.

Договор о предоставлении банковских услуг физическим лицам с использованием системы дистанционного банковского обслуживания (Договор) – договор, заключенный между Банком и Клиентом, устанавливающий правовые отношения между Банком и Клиентом при предоставлении Банком доступа к услугам, оказываемым с использованием Системы ДБО. Договор состоит из следующих неотъемлемых частей:

- **Заявление о присоединении** – заявление Клиента о присоединении к настоящим Правилам (по форме Приложения № 1 к настоящим Правилам).
- **Правила** – Правила дистанционного банковского обслуживания физических лиц в ООО КБ «РостФинанс», размещенные на сайте Банка www.rostfinance.ru в сети Интернет.

  При прохождении Клиентом самостоятельной регистрации в Системе ДБО для заключения Договора Заявление о присоединении не требуется.
- **Тарифы –** Сборник тарифов на услуги, предоставляемые ООО КБ «РостФинанс». Тарифы размещены для ознакомления на Сайте Банка по адресу https://www.rostfinance.ru

Идентификация – определение сотрудником Банка личности Клиента по предъявленному Клиентом документу, удостоверяющему личность, или определение Клиента Системой ДБО на основании Пароля/Логина, используемых при входе в Систему ДБО.

Идентификатор пользователя (Логин) – средство идентификации Клиента, представляющее собой уникальную последовательность символов, которая позволяет Банку идентифицировать владельца Логина и Пароля в Системе ДБО. Логин формируется Клиентом самостоятельно в Системе ДБО в момент подключения к Системе ДБО или Банком в момент подачи Заявления о присоединении (по форме Приложения № 1 к настоящим Правилам).

Канал доступа – информационно-телекоммуникационный канал общего доступа в сети «Интернет», поддерживаемый Системой ДБО.

Клиент – физическое лицо, с которым заключен Договор, имеющий Счет(а), открытый(ые) в Банке.

Компрометация Логина/Пароля и/или Одноразового пароля – утрата доверия к тому, что используемые Логин, Пароль и/или Одноразовый пароль обеспечивают безопасность информации, передаваемой Клиентом в Банк с использованием Системы ДБО.

Лимит на проведение операций – предельно допустимый размер денежных средств на проведение Операций через Систему ДБО.

Одноразовый пароль – средство подтверждения Клиентом неизменности, подлинности и целостности передаваемого по Системе ДБО Распоряжения, формируется Системой ДБО и направляется Клиенту на указанный им номер мобильного телефона посредством sms-сообщения/Push-уведомления для удостоверения права распоряжения средствами на счетах при совершении операций и является ПЭП Клиента в соответствии с Федеральным законом № 63-ФЗ.

Операция – операция, совершаемая Клиентом в Системе ДБО. В рамках настоящих Правил различают следующие виды операций:

– **Финансовая операция** – операция по распоряжению денежными средствами Клиента с помощью Системы ДБО, осуществляемая на основании Распоряжений Клиента, передаваемых посредством Системы ДБО в соответствии с условиями настоящих Правил и других договоров, заключенных между Банком и Клиентом.

– **Информационная операция** – предоставление Банком Клиенту информации о состоянии и использовании Счета/Карты Клиента, о проведенных операциях или иной информации, связанной с операциями, проведенными Клиентом в Банке.

– **Сервисная операция** – предоставление Клиенту возможности изменения Логина и/или Пароля, возможности отзыва неисполненного Банком Распоряжения, блокировки/разблокировки Карты.

– **Несанкционированная операция –** Финансовая операция, совершенная без согласия Клиента на ее совершение.

Пароль – средство аутентификации, служащее для подтверждения Клиентом своего права распоряжаться Счетами, представляет собой секретную последовательность символов, которая известна только Клиенту.

Представитель клиента (Представитель) – лицо (включая единоличный исполнительный орган юридического лица), совершающее операции (сделки) и/или операции с денежными средствами, полномочия которого подтверждены доверенностью, договором, законом либо актом уполномоченного на то государственного органа или органа местного самоуправления, в том числе лица, которым предоставлены полномочия по распоряжению банковским счетом (вкладом) с использованием технологии дистанционного банковского обслуживания.

Распоряжение – форма для создания Клиентом, посредством Системы ДБО, документа в электронном виде, подтверждения ЭД Одноразовым паролем и передачи по Каналам доступа Банку для совершения Операции.

Регистрация распоряжений – автоматическое внесение в электронной форме записи о получении Банком распоряжения Клиента в реестр распоряжений Системы ДБО, который формируется и ведется в Системе ДБО.

Сайт Банка – официальный сайт Банка в информационно-телекоммуникационной сети «Интернет» по адресу https://www.rostfinance.ru

Система ДБО – система дистанционного банковского обслуживания, обмена электронными документами, включающая комплекс программно-аппаратных средств и организационных мероприятий для составления, удостоверения, передачи и обработки ЭД по

телекоммуникационным каналам связи, используемым Клиентом и Банком. Банк предоставляет своим Клиентам ДБО с использованием Интернет-банка и/или Мобильного банка:

– ***Интернет-банк*** – сервис ДБО, позволяющий управлять Счетами в рублях и иностранной валюте, а также управлять другими продуктами Банка в режиме реального времени посредством сети Интернет.

– ***Мобильный банк*** – сервис ДБО, мобильное приложение, предоставляющее Клиенту возможность доступа к Интернет-банку, с использованием мобильного устройства на базе операционной системы iOS или Android.

Сторона(-ы) – Банк или Клиент, вместе или отдельно именуемые соответственно «Сторона», «Стороны».

Электронный документ (ЭД) – одна из форм представления распоряжений Клиента Банку в Системе ДБО. ЭД составляется в электронном виде и содержит все необходимые реквизиты, подписывается Одноразовым паролем Клиента, имеет равную юридическую силу с документами, составленными на бумажных носителях, подписанными собственноручной подписью Клиента, и является основанием для совершения операций по счетам или иных указанных в ЭД действий.

Любой удобный способ передачи письма/информации клиенту (далее- Любой удобный способ): передача письма непосредственно клиенту, его представителю в подразделении Банка (филиала); направление письма с использованием системы дистанционного банковского обслуживания, включая интернет-банкинга; направление телефонограммы с обязательным фиксированием информации в Журнале передачи телефонограмм согласно Приложению № 40 к настоящим Правилам; направление письма по электронной почте на электронный адрес клиента; направление заказного письма почтой России или экспресс-почтой; направление письма с использованием факсимильной связи.

2.Основные положения

2.1.Настоящие Правила регулируют порядок и условия предоставления Банком услуг с использованием Системы ДБО, включая порядок подключения Клиента к Системе ДБО, порядок обмена ЭД между Сторонами в целях выполнения обязательств по договору текущего счета/договору вклада/договору текущего счета с использованием банковских карт, заключенным между Банком и Клиентом, в также определяют права, обязанности и ответственность Сторон, возникающие в этой связи.

2.2.Настоящие Правила являются публичной офертой Банка. Действующая редакция настоящих Правил размещается на Сайте Банка и в офисе Банка. По просьбе Клиента сотрудник Банка обязан предоставить в удобном Клиенту виде действующую редакцию настоящих Правил.

2.3.Настоящие Правила разработаны в соответствии с действующим законодательством Российской Федерации и национальными стандартами Российской Федерации в части обеспечения информационной безопасности и защиты информации, требованиями Банка России, требованиями Федеральных служб, уполномоченных в области безопасности, надзора в сфере связи, информационных технологий и массовых коммуникаций, в том числе:

– Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» (Федеральный закон № 63-ФЗ);

– Федеральным законом от 27.06.2011 № 161-ФЗ «О национальной платежной системе»;

– Федеральным законом от 02.12.1990 № 395-1 «О банках и банковской деятельности»;

– Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (Федеральный закон № 115-ФЗ);

– Федеральный закон от 10.12.2003 № 173-ФЗ «О валютном регулировании и

валютном контроле» (Федеральный закон № 173-ФЗ);

– Федеральный закон от 23.12.2003 № 177-ФЗ «О страховании вкладов в банках Российской Федерации»;

– Положением Банка России от 09.06.2012 № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»;

– Положением Банка России от 19.06.2012 № 383-П «О правилах осуществления перевода денежных средств»;

– Положением Банка России от 17.04.2019 № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»;

– Инструкции Банка России от 30.05.2014 № 153-И «Об открытии и закрытии банковских счетов, счетов по вкладам (депозитам), депозитных счетов» (Инструкция Банка России № 153-И).

2.4. Настоящие Правила также распространяются на все правоотношения с Клиентом, возникшие до введения в действие настоящих Правил, касающиеся дистанционного банковского обслуживания физического лица в Системе ДБО.

2.5.Договор заключается только с Клиентом, находящимся на обслуживании в Банке на основании заключенного с Банком договора текущего счета/договора вклада/договора текущего счета с использованием банковских карт.

2.6.Заключение Договора для подключения к Системе ДБО осуществляется способом присоединения Клиента к настоящим Правилам. Присоединение Клиента к части Правил, а также внесение Клиентом изменений и/или дополнений в текст настоящих Правил не предусматривается.

2.7.До заключения Договора Клиент обязан представить Банку достоверные сведения и информацию, предусмотренные действующим законодательством Российской Федерации, Общими правилами и договором текущего счета/договором вклада/договором текущего счета с использованием банковской карты, соответственно. В случае изменения сведений и информации, предоставленных Банку ранее, Клиент должен представить сведения и информацию актуальные на дату заключения Договора.

2.8.На основании заключенного Договора, Клиенту предоставляется доступ ко всем Счетам, открытым Клиентом в Банке на момент подачи Заявления о присоединении или прохождения самостоятельной регистрации в Системе ДБО. Все вновь открытые Клиентом Счета подключаются к Системе ДБО без дополнительных заявлений Клиента.

2.9.Не допускается заключение Договора в пользу третьего лица. Не допускается уступка прав, принадлежащих Клиенту по Договору.

2.10.За обслуживание и использование Системы ДБО, совершение Операций в Системе ДБО Банк взимает комиссионное вознаграждение в соответствии с Тарифами.

2.11.Банк с целью ознакомления Клиентов с условиями Правил и Тарифов размещает Правила и Тарифы путем опубликования информации одним или несколькими из нижеперечисленных способов:

- размещение такой информации на Сайте Банка в сети Интернет www.rostfinance.ru;
- оповещение Клиентов через Систему ДБО;
- размещение объявлений на информационных стендах в подразделениях Банка, осуществляющих обслуживание Клиентов;
- иные способы, позволяющие Клиенту получить информацию и установить, что она исходит от Банка.

2.12.Моментом ознакомления Клиента с опубликованной информацией считается

момент, с которого информация доступна для Клиентов.

2.13.Клиент предоставляет Банку право списывать без дополнительных распоряжений Клиента (заранее данный акцепт) с любых Счетов Клиента в Банке комиссионное вознаграждение за оказанные услуги по Договору в соответствии с Тарифами Банка, а также другие расходы, понесенные Банком, в том числе комиссионные вознаграждения, выплачиваемые Банком третьим лицам, стоимость телефонных переговоров, факсимильных сообщений и почтовых отправлений, связанных с обслуживанием Клиента в Системе ДБО, за исключением случаев, когда такие списания противоречат условиям договора соответствующего счета.

2.14.Все операции в Системе ДБО отражаются по московскому времени.

2.15.Стороны договорились об использовании Системы ДБО для обмена между ними ЭД с применением ПЭП для совершения Операций в соответствии с действующим законодательством Российской Федерации.

2.16.Клиент признает, что информационная безопасность Системы ДБО и алгоритмы достаточны для подтверждения подлинности, целостности и авторства Распоряжений (включая созданные Клиентом и принятые Банком ЭД).

2.17.Клиент поставлен в известность и в полной мере осознает, что передача конфиденциальной информации по Каналам доступа влечет риск несанкционированного доступа к такой информации третьих лиц.

2.18.В случае, когда передача конфиденциальной информации по Каналам доступа осуществляется по требованию или в соответствии с Распоряжением Клиента, Банк не несет ответственности за несанкционированный доступ третьих лиц к такой информации при ее передаче.

2.19.Банком предпринимаются все возможные меры для обеспечения безопасности и защиты информации Клиента от несанкционированных попыток доступа, изменения, раскрытия или уничтожения, а также иных видов ненадлежащего использования.

2.20.В целях оказания услуг ДБО Банк поручает ЗАО «Биллинговый центр» (адрес: 630055, Новосибирская область, г. Новосибирск, ул. Мусы Джалиля, дом 11, офис 218) обработку персональных данных Клиента, указанных в Заявлении о присоединении, на срок действия договора.

3.Порядок заключения договора о предоставлении банковских услуг физическим лицам с использованием системы дистанционного банковского обслуживания

3.1.Заключение Договора для первоначального подключения к Системе ДБО осуществляется путем присоединения Клиента к настоящим Правилам любым нижеперечисленным способом:

3.1.1.путем личного обращения Клиента в офис Банка с Заявлением о присоединении;

3.1.2.путем самостоятельной регистрации и подключения к Системе ДБО;

3.1.3.путем указания необходимости предоставления доступа к Системе ДБО в «Заявлении на получение личных банковских карт MasterCard ООО КБ «РостФинанс» и открытие специального карточного счета (СКС).

3.2.Для заключения Договора способом, указанным в п. 3.1.1 настоящих Правил, Клиент предоставляет в офис Банка надлежащим образом заполненное и подписанное Заявление о присоединении по форме Приложения № 1 к настоящим Правилам в 2 (двух) экземплярах.

Договор считается заключенным с момента проставления уполномоченным сотрудником Банка на бумажном носителе Заявления о присоединении соответствующей отметки о приеме.

Дата приема Банком Заявления о присоединении является датой заключения Договора.

3.3.Для заключения Договора способом, указанным в п. 3.1.2 настоящих Правил, Клиент проходит самостоятельную регистрацию в Системе ДБО.

Для самостоятельной регистрации необходимо осуществить следующие действия:

3.3.1.По ссылке на Сайте Банка или в мобильном приложении заполнить форму регистрации и ввести уникальные данные, позволяющие однозначно установить наличие договорных отношений Клиента с Банком: фамилию, имя, отчество, а также сведения о номере Счета и/или номере Карты и/или реквизиты документа, удостоверяющего личность и иную информацию, указанную в полях регистрационной формы;

3.3.2.Самостоятельно создать Логин, используя разрешенные символы, и направить в Банк запрос на получение Временного пароля. В ответ на полученный запрос Клиенту направляется Временный пароль, сформированный Банком, в виде sms-сообщения на номер мобильного телефона, предоставленный Клиентом при открытии Счета. Действие Временного пароля ограничено Системой ДБО по времени использования и требует обязательной смены его на постоянный Пароль;

3.3.3.Для доступа в Систему ДБО Клиент вводит самостоятельно им сформированный Логин и полученный от Банка в виде sms-сообщения Временный пароль на Сайте Банка. После ввода указанных данных Система ДБО предлагает Клиенту сформировать постоянный Пароль, который позволяет провести Аутентификацию Клиента в Системе ДБО.

Вход Клиентом в Систему ДБО с применением постоянного Пароля и Аутентификация Клиента Банком признается согласием Клиента на присоединение к настоящим Правилам и заключение Договора.

Договор считается заключенным с момента завершения регистрации Клиента в Системе ДБО.

3.4.Банк считает достаточным основанием полагать, что Договор заключен непосредственно с Клиентом, если лицом, обратившемся за получением услуги ДБО, были предоставлены в Банк все необходимые сведения, указанные в п. 2.7 настоящих Правил, а также введен Временный пароль, направленный в виде sms-сообщения на номер мобильного телефона Клиента. Риск убытков и иных неблагоприятных последствий вследствие доступа третьих лиц к сведениям, необходимым для самостоятельной регистрации в Системе ДБО, а также к номеру мобильного телефона Клиента и/или Логину, Паролю, несет Клиент.

3.5.Доступ к Системе ДБО предоставляется Клиентам, заключившим Договор с Банком и подключенным к Системе ДБО в соответствии с настоящими Правилами, не позднее рабочего дня, следующего за днем заключения Договора.

4.Порядок доступа и работы в системе дистанционного банковского обслуживания

4.1.Банк предоставляет Клиенту доступ к Системе ДБО для совершения Финансовых и/или Информационных и/или Сервисных операций, принимает к исполнению Распоряжения Клиента только при условии выполнения Идентификации Клиента с помощью предусмотренных Договором Логина, Пароля и Одноразового пароля.

4.2.Доступ Клиента в Систему ДБО осуществляется после выполнения Банком процедуры Идентификации Клиента при входе в Интернет-банк.

4.3.Вход Клиента в Интернет-банк осуществляется через web-браузер поддерживающий работу Системы ДБО или через сервис Мобильный банк после загрузки приложения на мобильное устройство (телефон, планшет).

Мобильное приложение для доступа в Систему ДБО с использованием сервиса Мобильный банк может быть загружено Клиентом самостоятельно из:

–официального магазина приложений Apple (для владельцев устройств на платформе

iOS);

–официального магазина приложений Android (для владельцев устройств, работающих на платформе Android).

4.4.Средством Идентификации Клиента при входе в Систему ДБО является Логин, указанный в Заявлении о присоединении при заключении Договора в офисе Банка или созданный Клиентом самостоятельно при регистрации в Системе ДБО на Сайте Банка.

4.5.Средством Аутентификации Клиента при входе в Систему ДБО является Пароль.

В случае превышения лимита попыток неверного ввода Клиентом Логина и/или Пароля при входе в Систему ДБО доступ в Систему ДБО автоматически блокируется.

Автоматическая блокировка производится Системой ДБО после 3 (трех) неудачных попыток ввода Логина/Пароля на вход в систему ДБО и снимается по истечении 3 (трех) минут для повторного ввода. Если Клиент не может воспроизвести Логин/Пароль, то ему необходимо восстановить его самостоятельно при помощи функции Системы ДБО или обращения в службу поддержки ДБО Банка.

4.6.Банк вправе приостановить использование Клиентом Пароля на основании требования Клиента, переданного способом, позволяющим Банку установить, что требование исходит от Клиента, а также в случае наличия у Банка оснований считать, что возможно несанкционированное использование Системы ДБО от имени Клиента.

4.7.Банк уведомляет Клиента о факте приостановлении или прекращении использования Системы ДБО с указанием причины такого приостановления или прекращения – в день приостановления (прекращения) использования Системы ДБО. Уведомление осуществляется направление SMS-сообщений / PUSH-уведомлений на номер мобильного телефона, указанный Клиентом. В SMS-сообщениях / PUSH – уведомлениях указываются – дата, причины такого приостановления (прекращения) и другие данные по усмотрению Банка.

4.8.Для подтверждения Клиентом Финансовых операций, а также отправки информационных сообщений в Банк в качестве методов формирования и проверки Электронной подписи используются методы, основанные на применении разовых паролей, выступающих в качестве одноразовых Ключей электронной подписи и одноразовых Ключей проверки электронной подписи. Одноразовый пароль, направляется в виде sms-сообщения на номер мобильного телефона Клиента, указанный Клиентом в Заявлении о присоединении (при заключении Договора в офисе Банка) или предоставленный Клиентом ранее при открытии Счета (при самостоятельной регистрации в Системе ДБО).

4.9.Клиент обязан проверять текст sms-сообщения, содержащий Одноразовый пароль, а также краткую информацию о совершаемой Операции. Клиент не должен подтверждать Операцию Одноразовым паролем, если информация в sms-сообщении не совпадает с Финансовой операцией, которую ему необходимо подтвердить.

4.10.Клиент вправе приостановить использование им Системы ДБО, подав в Банк Заявление об изменении доступа к системе дистанционного банковского обслуживания (по форме Приложения № 2 к настоящим Правилам).

4.11.Для возобновления использования Системы ДБО, приостановленного по инициативе Клиента, Клиент может воспользоваться сервисом восстановления Пароля в системе ДБО или обратиться в офис Банка с Заявлением об изменении доступа к Системе ДБО.

4.12.Возобновление использования Клиентом Системы ДБО осуществляется Банком не позднее рабочего дня, следующего за днем подачи Клиентом Заявления об изменении доступа к Системе ДБО.

5.Порядок проведения операций

5.1.В Системе ДБО Банк предоставляет доступ к текущим счетам Клиента, текущим счетам Клиента с использованием международных пластиковых карт, счетам по вкладам (депозитам), кредитам, а также другим услугам Банка.

5.2.Все операции осуществляются в пределах остатка денежных средств на счете Клиента с одновременным соблюдением Лимита на сумму проводимых операций. Ограничение на осуществление операций по счетам клиентов указаны в Приложении №3 к настоящим Правилам.

5.3.Для выполнения Финансовой операции с помощью Системы ДБО Клиент заполняет стандартную форму распоряжения в Системе ДБО, подписывает Распоряжение Одноразовым паролем и производит отправку Распоряжения в Банк.

5.4.Не подписанное Одноразовым паролем Распоряжение не регистрируется, и считается, что Клиент отказался от передачи Распоряжения, даже если им были произведены все остальные действия, необходимые для его передачи.

5.5.Моментом поступления в Банк Распоряжения считается момент регистрации Распоряжения с внесением времени и даты записи Распоряжения в реестр распоряжений Системы ДБО. Время определяется по времени системных часов аппаратных средств Банка, настроенных на московское время.

5.6.В случае, если по каким-либо не зависящим от Банка и/или Клиента причинам (разрыв связи и тому подобное), Клиент не получил подтверждение о регистрации Распоряжения либо уведомление об отказе в регистрации Распоряжения, ответственность за установление окончательного результата передачи Распоряжения возлагается на Клиента.

5.7.Клиент и Банк признают, что ЭД в Системе ДБО, удостоверенные Одноразовым паролем:

5.7.1.Равнозначны, в том числе имеют равную юридическую и доказательную силу с аналогичными по содержанию и смыслу расчетными документами, подписанными собственноручной подписью Клиента;

5.7.2.Не могут быть оспорены Банком, Клиентом и третьими лицами, или быть признаны недействительными по основанию, что они переданы в Банк с использованием Системы ДБО через сеть «Интернет», или составлены в электронной форме;

5.7.3.Могут использоваться в качестве доказательства в суде и в других государственных, и негосударственных органах, и организациях;

5.7.4.Достаточным и надлежащим образом удостоверяют право Клиента распоряжаться средствами, размещенными на счетах Клиента, подключенных к Системе ДБО.

5.8.Стороны признают, что переданные Банком Информационные операции, в том числе содержащие в установленных настоящими Правилами случаях электронные и иные средства, используемые Банком для подтверждения подлинности и/или неизменности и целостности направляемых Клиенту информационных сообщений, признаются равными по юридической силе соответствующим документам в письменном виде, подписанным уполномоченными лицами, оформляемым при совершении аналогичных операций в Банке лично Клиентом, и порождают аналогичные им права и обязанности сторон и могут служить доказательством в суде.

5.9.Распоряжения Клиентов на выполнение Операций по Счету(ам) исполняются в соответствии со сроками выполнения Распоряжений Клиентов, установленными действующим законодательством Российской Федерации для распоряжений такого рода. Банк вправе исполнять отдельные распоряжения Клиентов в режиме реального времени.

5.10.Банк вправе отказаться от исполнения зарегистрированного Распоряжения в следующих случаях:

5.10.1.Проводимая Операция не соответствует режиму счета и/или исполнение Распоряжения повлекло бы нарушение условий/соглашений, заключенных между Банком и Клиентом;

5.10.2.Распоряжение противоречит действующему законодательству Российской Федерации, настоящим Правилам, нормативным актам Банка России и/или внутренним документам Банка;

5.10.3.По основаниям, предусмотренным Федеральным законом № 115-ФЗ и

Федеральным законом № 173-ФЗ.

5.10.4.Если до исполнения Распоряжения Банком от Клиента получена информация о техническом сбое, в соответствии с п. 5.6 настоящих Правил.

5.11.Клиент имеет право направить в Банк запрос на отзыв ЭД в день его отправки. Банк принимает отзыв ЭД только в том случае, если ЭД оформлен как перевод по произвольным реквизитам (где Клиент вводит реквизиты получателя самостоятельно), еще не исполнен и Банк имеет возможность отменить его исполнение.

5.12.Клиент несет полную ответственность за правильность реквизитов Операции, указанных им при ее проведении. В случае если Операция была произведена Банком по реквизитам, ошибочно указанным Клиентом, Клиент самостоятельно обращается к получателю платежа с целью возврата денежных средств или в кредитную организацию, обслуживающую получателя перевода.

5.13.При выполнении Операций, связанных с переводами денежных средств между счетами, открытыми в разных валютах, Банком производится конвертация денежных средств по курсу Банка, установленного на момент выполнения операции. Информация о курсах валют доводится до Клиента путем размещения их на официальном сайт Банка в информационно-телекоммуникационной сети «Интернет» по адресу https://www.rostfinance.ru и системе ДБО.

5.14.Банк исполняет Информационные операции по счету Клиента на основании полученных и принятых к исполнению Распоряжений Клиента. Указанные Распоряжения передаются Клиентом Банку с использованием Канала доступа. Наличие в Банке ЭД Клиента, содержащего распоряжение Клиента на исполнение Информационной операции и надлежащим образом в соответствии с настоящими Правилами подтвержденного Одноразовым паролем, является для Банка достаточным основанием (если иное не предусмотрено настоящими Правилами) для осуществления Информационной операции.

5.15.Распоряжения Клиентов на проведение Информационных операций исполняются в режиме реального времени при наличии технической возможности.

5.16.Банк вправе в любой момент потребовать от Клиента подписание документов на бумажном носителе, эквивалентных по смыслу и содержанию, переданным Клиентом и зарегистрированным Банком Распоряжениям.

6.Порядок уведомления клиента об операциях, совершенных по счету с использованием системы дистанционного банковского обслуживания

6.1.В соответствии с законодательством Российской Федерации Банк уведомляет Клиента о расходных операциях по его Счетам. Уведомление Клиента о списании средств со Счета либо отказе в совершении Операции по Счету осуществляется путем установления в Системе ДБО статуса расчетного документа «Принят банком» / «Исполнен» / «Возвращен».

Клиент согласен с тем, что присвоение статуса «Исполнен» в Системе ДБО является надлежащим уведомлением Банком Клиента о совершении Банком соответствующей Операции по Счету.

6.2.Клиент вправе выбрать в качестве дополнительного способа уведомления об Операциях, совершенных по Счету(ам) с использованием Системы ДБО, любой нижеперечисленный способ:

6.2.1.Посредством направления sms-сообщений на номер мобильного телефона Клиента (при условии наличия у Клиента подключенного Мобильного банка, sms-уведомления подключаются Клиентом самостоятельно в Мобильном банке);

6.2.2.Посредством направления Push-уведомлений (при условии наличия у Клиента подключенного Мобильного банка, Push-уведомления подключаются Клиентом самостоятельно в Мобильном банке);

6.3.Уведомление о совершенной Операции с использованием Системы ДБО считается

полученным Клиентом:

–в момент доступа Клиента к Системе ДБО, зафиксированного программным обеспечением Банка;

–с момента отправления sms-сообщения, указанного в п. 6.2.1 настоящих Правил, зафиксированного программным обеспечением Банка;

–с момента отправления Push-уведомления, указанного в п. 6.2.2 настоящих Правил, на мобильное устройство Клиента;

6.4.Клиент обязан предоставить Банку достоверную информацию для получения уведомлений о совершенной Операции с использованием Системы ДБО, при изменении информации, указанной в настоящем пункте, своевременно предоставить в Банк обновленную информацию.

6.5.Клиент вправе выбрать один из нескольких способов получения уведомлений об Операциях, совершенных по Счету(ам) с использованием Системы ДБО, из предложенных Банком, а также в любой момент изменить способ получения уведомлений, подав в Банк Заявление об изменении доступа к Системе ДБО.

6.6.Уведомление об Операциях, совершенных по Счету(ам) с использованием Системы ДБО, способом, указанным в п. 6.1 настоящих Правил, осуществляется без взимания Банком комиссионного вознаграждения. За предоставление уведомлений способом, указанным в п. 6.2 настоящих Правил, Банк вправе взимать вознаграждение в соответствии с Тарифами.

6.7.В целях снижения рисков Несанкционированных операций, совершенных по Счету(ам) с использованием Системы ДБО, Клиенту необходимо своевременно знакомиться с уведомлениями, пришедшими на номер мобильного телефона и/или осуществлять доступ к Системе ДБО.

6.8.Клиент обеспечивает наличие в Банке контактной информации о номере мобильного телефона, необходимой для направления уведомлений о совершении Операций по Счету(ам) с использованием Системы ДБО и поддерживает их в актуальном состоянии.

6.9.В случае изменения номера мобильного телефона, предоставленного в Банк для получения Клиентом уведомлений об Операциях, совершенных по Счету(ам) с использованием Системы ДБО, Клиент своевременно представляет в Банк измененную информацию.

Изменение информации о номере мобильного телефона производится путем подачи в Банк письменного заявления на бумажном носителе по форме Приложения №2 «Заявление об изменении доступа к Системе ДБО» в офис Банка и/или в виде Информационной операции по Системе ДБО.

До момента предоставления Клиентом в Банк изменений контактной информации способом, указанным в настоящем пункте, Клиент принимает на себя риски, связанные с непредставлением Банку информации об изменении номера мобильного телефона.

6.10.Клиент должен содержать технические средства (мобильный телефон, ноутбук, компьютер, планшет и т.д.), обеспечивающие возможность получения от Банка уведомлений о совершении каждой Операции по Счету(ам) с использованием Системы ДБО в исправном рабочем состоянии. В случае неисправности указанных технических средств, Клиент принимает на себя риски, связанные с неполучением от Банка уведомлений о совершении Операций по Счету(ам) с использованием Системы ДБО.

6.11.Клиент самостоятельно и за свой счет обеспечивает и оплачивает технические, программные и коммуникационные ресурсы, необходимые для организации получения направляемых Банком уведомлений о совершении Операций с использованием Системы ДБО.

7.Компрометация логина/пароля, одноразового пароля

7.1.В случае Компрометации Логина, Пароля и/или Одноразового пароля (в том числе утраты, незаконного использования третьими лицами и т.д.) и/или их использования без согласия

Клиента, совершения Несанкционированной операции Клиент обязан направить уведомление в Банк незамедлительно после обнаружения факта Компрометации Логина/Пароля/Одноразового пароля, и/или их использования без согласия Клиента, и/или совершения Несанкционированной операции, не позднее дня, следующего за днем получения от Банка уведомления о Финансовой операции, совершенной по Счету с использованием Системы ДБО.

До момента поступления в Банк уведомления о Компрометации Логина/Пароля и /или Одноразового пароля (в том числе утраты, незаконного использования третьими лицами и т.д.) и/или их использования без согласия Клиента, совершении Несанкционированной операции ответственность по Операциям, совершенным по Счету с использованием Системы ДБО, несет Клиент.

7.2.Клиент уведомляет Банк о Компрометации Логина/Пароля и/или Одноразового пароля (в том числе утраты, незаконного использования третьими лицами и т. д.) и/или их использовании без согласия Клиента, совершения Несанкционированной операции любым из следующих способов:

7.2.1.По номеру телефона, опубликованному на Сайте Банка.

7.2.2.В виде письменного заявления на бумажном носителе, переданного Клиентом в офис Банка.

При поступлении уведомлений о Компрометации Логина/Пароля и/или Одноразового пароля (в том числе утраты, незаконного использования третьими лицами и т.д.) и/или их использования без согласия Клиента способами, указанными в п. 7.2.1 – **Ошибка! Источник ссылки не найден.** настоящих Правил, в течение 3 (трех) рабочих дней Клиент обязан представить в Банк оригинал заявления на бумажном носителе.

7.3.После получения любым из перечисленных в п. 7.2 способов от Клиента уведомления о Компрометации Логина/Пароля и/или Одноразового пароля (в том числе утраты, незаконного использования третьими лицами и т.д.) и/или их использования без согласия Клиента Банк приостанавливает использование Клиентом Системы ДБО, после чего прекращается возможность совершения Клиентом Операций по Счету с использованием Системы ДБО. Приостановление работы Клиента в Системе ДБО не прекращает обязательств Клиента и Банка, возникших до момента ее приостановления.

7.4.Формирование нового Логина осуществляется в офисе Банка на основании Заявления об изменении доступа к Системе ДБО либо Клиентом самостоятельно на Сайте Банка. Восстановление Пароля осуществляется в Системе ДБО.

7.5.Банк возобновляет работу Клиента в Системе ДБО на основании заявления Клиента, составленного на бумажном носителе, не позднее рабочего дня, следующего за днем получения такого заявления, либо на основании самостоятельных действий, осуществленных Клиентом на Сайте Банка.

7.6.При получении от Клиента уведомления, указанного в пункте 7.1 настоящих Правил, после осуществления списания денежных средств со Счета Банк незамедлительно направляет в кредитную организацию, обслуживающую получателя средств, уведомление о приостановлении зачисления денежных средств на счет получателя по форме и в порядке, которые установлены нормативным актом Банка России.

7.7.В случае выявления Банком Финансовой операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента, Банк на срок не более 2 (двух) рабочих дней приостанавливает исполнение соответствующего распоряжения о списании денежных средств со Счета Клиента, а также приостанавливает использование Системы ДБО.

7.7.1.О данном факте Банк незамедлительно информирует Клиента и запрашивает у Клиента подтверждение возобновления исполнения.

Одновременно с извещением Банк предоставляет Клиенту рекомендации по снижению рисков повторного осуществления перевода денежных средств без согласия Клиента.

7.7.2.При получении от Клиента подтверждения возобновления исполнения распоряжения Банк незамедлительно возобновляет исполнение распоряжения и возобновляет

действие доступа в Систему ДБО.

7.7.3.При получении от Клиента отказа возобновления исполнения распоряжения (сообщения о операции без согласия клиента) Банк незамедлительно отменяет исполнение распоряжения и не возобновляет действие доступа в Систему ДБО.

7.8.При неполучении от Клиента подтверждения Банк возобновляет исполнение распоряжения и возобновляет действие доступа в Систему ДБО по истечении 2 (двух) рабочих дней после совершения Банком действий, предусмотренных п. 7.7 настоящих Правил.

8.Права и обязанности Банка

8.1.Банк обязуется:

8.1.1.Не позднее рабочего дня, следующего за днем присоединения Клиента к настоящим Правилам путем подачи Заявления о присоединении в офис Банка, предоставить Клиенту доступ к Системе ДБО и сообщить ему Логин и Временный пароль в определенном настоящим Правилами порядке.

8.1.2.Принять все необходимые меры организационного и технического характера для обеспечения режима конфиденциальности в отношении Логина Клиента до сообщения его Клиенту, в случае подачи Заявления о присоединении в офис Банка, а также обеспечить невозможность доступа посторонних лиц к информации о Логинах и Паролях, находящейся в распоряжении Банка.

8.1.3.Принять меры для предотвращения несанкционированного доступа третьих лиц к конфиденциальной информации, связанной с использованием Системы ДБО. Любая информация такого рода может быть предоставлена третьим лицам в порядке, установленном действующим законодательством Российской Федерации.

8.1.4.В случае, когда использование Логина и/или Пароля предполагает передачу Клиенту либо хранение Банком какой-либо конфиденциальной информации, принять все необходимые меры организационного и технического характера для предотвращения доступа третьих лиц к конфиденциальной информации до передачи ее Клиенту, а также во время хранения.

8.1.5.Предоставлять Клиенту документы, актуальную и достоверную информацию о переданных Клиентом ЭД, проведенных Операциях по его Счету(ам) с использованием Системы ДБО.

8.1.6.Уведомлять Клиентов об изменении и/или дополнении Тарифов и/или Правил не позднее, чем за 10 (десять) рабочих дней до даты введения в действие новых Тарифов Банка и/или новой редакции настоящих Правил путем размещения соответствующих изменений и дополнений или новых редакций указанных документов на стойках/стенде размещенных в офисе Банка и на Сайте Банка.

8.1.7.Регистрировать и хранить в течение не менее 5 лет протоколы действий Клиента в Системе ДБО. Протоколы операций Клиента имеют гриф «Конфиденциально» и являются конфиденциальной информацией Банка. В случае компрометации ключевой информации Системы ДБО Банк имеет право отказать Клиенту в предоставлении данной информации по письменному или устному заявлению Клиента. Протоколы операций могут быть выданы только по решению суда либо по письменному запросу правоохранительных органов при урегулировании споров.

8.1.8.Аннулировать совершение приостановленного перевода денежных средств, выявленного в ходе мониторинга операций, соответствующих признакам совершения перевода денежных средств без согласия клиента, если клиент опроверг легитимность операции.

8.1.9.Отменить приостановку использование Клиентом Системы ДБО при подтверждении Клиентом операции, соответствующей признакам совершения перевода денежных средств без согласия клиента.

8.1.10.С целью реализации ограничений по параметрам операций по осуществлению

переводов денежных средств, применить ограничения на максимальную сумму перевода денежных средств за одну операцию и (или) за определенный период времени либо (и) ограничения на перечень возможных получателей денежных средств на основании поданного в Банк от Клиента заявления в порядке, предусмотренном пунктом 9.2.5. настоящих Правил.

8.2.Банк имеет право:

8.2.1.Отказать в заключение Договора и представлении банковского обслуживания, в случае если Клиентом в Банк не представлены все требуемые для заключения Договора документы, контактный номер мобильного телефона и/или адрес электронной почты, либо представлены недостоверные документы и информация, а также в иных случаях, предусмотренных законодательством Российской Федерации.

8.2.2.Отказать в заключение Договора в случае если при проведении Клиентом самостоятельной регистрации в Системе ДБО, у Банка возникли подозрения в том, что за заключением Договора обратилось ненадлежащее лицо, располагающее сведениями о Клиенте и его отношениях с Банком. При этом Клиент имеет право заключить Договор путем личного обращения в офис Банка.

8.2.3.Проверять любую информацию о Клиенте, которую Банк сочтет необходимой для надлежащего исполнения им своих обязательств в рамках настоящих Правил, любыми способами и средствами, не противоречащими действующему законодательству Российской Федерации.

8.2.4.Приостановить или прекратить доступ Клиента в Систему ДБО в следующих случаях:

8.2.4.1. нарушения Клиентом условий настоящих Правил, Договора и (или) договора текущего счета/договора вклада/договора текущего счета с использованием банковской карты;

8.2.4.2. несоблюдения Клиентом правил и рекомендаций по обеспечению безопасности, определенных настоящими Правилами и Памяткой о мерах по безопасному использованию электронного средства платежа;

8.2.4.3. обнаружения Банком Несанкционированных Операций с использованием Системы ДБО, а также в случае получения уведомления о Компрометации Логина/Пароля и/или Одноразового пароля подтверждения (в том числе утраты, незаконного использования третьими лицами и т.д.) и/или их использования без согласия Клиента;

8.2.4.4. недостаточности средств на Счете, с которого Банком удерживается плата за услуги ДБО в соответствии с Тарифами, для единовременного полного списания платы в соответствии с Тарифами;

8.2.4.5. непредставления Клиентом документов, необходимых для фиксирования информации в соответствии с нормами действующего законодательства, в течение 7 рабочих дней с даты направления запроса Банком Любым удобным способом;

8.2.4.6. в случае непредставления сведений и/или документов по запросу Банка в целях обновления сведений, полученных при идентификации Клиента, его представителя, бенефициарного владельца и выгодоприобретателя (при его наличии);

8.2.4.7.в случае, если у работников Банка, возникают подозрения, что операции по счетам Клиента в Банке совершается в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма. В этом случае Банк будет принимать только надлежащим образом оформленные расчетные документы на бумажном носителе.

8.2.4.8. по иным основаниям в соответствии с Федеральным законом № 115-ФЗ.

8.2.5.Отказать/приостановить выполнения Распоряжения Клиента о совершении Операции в случае:

8.2.5.1. не подтверждения Распоряжения Клиентом;

8.2.5.2. выявления Банком Финансовой операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента;

8.2.5.3. недостаточности денежных средств на Счете Клиента для исполнения Распоряжения;

8.2.5.4. недостаточности денежных средств на Счете Клиента для списания комиссионного вознаграждения;

8.2.5.5. превышение установленного лимита на проведение операций.

8.2.6.Отказать в выполнении распоряжения Клиента о совершении Операции, за исключением Операций по зачислению денежных средств, поступивших на Счет, по которой не представлены документы, необходимые для фиксирования информации в соответствии с положениями Федерального закона №115-ФЗ, а также в случае, если в результате реализации правил внутреннего контроля у работников Банка возникают подозрения, что Операции совершаются в целях легализации (отмывания) доходов, полученных преступным путем, финансированию терроризма.

8.2.7.Ограничить перечень видов Финансовых и Информационных операций, а также устанавливать и/или изменять лимиты на проведение операций, осуществляемых через Систему ДБО.

8.2.8.Отказать в возобновлении использования Клиентом Системы ДБО, приостановленного как по инициативе Банка, так и по инициативе Клиента, без объяснения причин.

8.2.9.Изменять и дополнять в одностороннем порядке настоящие Правила и/или Тарифы, за исключением случаев, когда одностороннее изменение Банком условий Правил/Тарифов запрещено законодательством Российской Федерации.

9.Права и обязанности клиента

9.1.Клиент обязуется:

9.1.1.Строго соблюдать условия настоящих Правил.

9.1.2.Своевременно оплачивать Банку комиссии и иные вознаграждения в соответствии с действующими Тарифами.

9.1.3.Изменить Временный пароль при первом входе в Систему ДБО.

9.1.4.Осуществлять контроль за Операциями по Счету(ам) в целях своевременного выявления и предупреждения совершения Несанкционированных операций путем получения и оперативной проверки уведомления, получаемого от Банка.

9.1.5.Самостоятельно и за свой счет обеспечить доступ в сеть «Интернет» для пользования услугами Банка с использованием Системы ДБО.

9.1.6.Письменно информировать Банк об изменении сведений, указанных Клиентом в Заявлении о присоединении, в течение 3 (трех) рабочих дней с даты изменений.

9.1.7.Ознакомиться с Памяткой о мерах по безопасному использованию электронного средства платежа, размещенной на Сайте Банка, соблюдать требования, изложенные в ней, а также соблюдать иные рекомендаций по информационной безопасности направленные Банком по Системе ДБО или иным способом, установленным настоящими Правилами.

9.1.8.Самостоятельно обеспечить хранение Логина/Пароля и/или Одноразового пароля способом, делающим их недоступными третьим лицам, а также немедленно уведомлять Банк об их компрометации.

9.1.9.Представлять документы и сведения по запросу Банка, необходимые Банку для осуществления функций, возложенных на него законодательством Российской Федерации.

9.1.10.Знакомиться, не реже одного раза в неделю, с текущей редакцией Правил и/или Тарифов, следить за изменениями и/или дополнениями, вносимыми Банком в Правила и/или Тарифы. Проведение операции в Системе ДБО Клиентом, ознакомившимся с Правилами и Тарифами, на Сайте Банка в день ее проведения, свидетельствует о принятии Клиентом условий

Правил и Тарифов с учетом всех изменений и дополнений, действующих на дату проведения Операции.

9.1.11.Знакомиться в системе ДБО с входящей корреспонденцией от Банка не реже 1 раза в календарный день.

9.2.Клиент имеет право:

9.2.1.Осуществлять операции в Системе ДБО в рамках настоящих Правил.

9.2.2.Неоднократно проверять статусы направленных в Банк ЭД и формировать выписки по Операциям.

9.2.3.Приостановить/возобновить использование им Системы ДБО в порядке, установленном настоящими Правилами.

9.2.4.Расторгнуть Договор в порядке, установленном настоящими Правилами, в том числе в случае несогласия с изменениями/дополнениями, внесенными в Правила и/или Тарифы.

9.2.5.Подать в Банк заявление в произвольной форме об установлении по инициативе Клиента ограничений на максимальную сумму перевода денежных средств за одну операцию и (или) за определенный период времени либо (и) об установлении по инициативе Клиента ограничений на перечень возможных получателей денежных средств.

10.Ответственность сторон

10.1.Стороны несут ответственность за неисполнение или ненадлежащее исполнение своих обязательств по Договору в соответствии с действующим законодательством Российской Федерации. Причинение убытков, вызванных неисполнением либо ненадлежащим исполнением этих обязательств, влечет за собой их возмещение виновной стороной в полном объеме.

10.2.Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение принятых по Договору обязательств на период действия обстоятельств непреодолимой силы и их последствий. К таким обстоятельствам относятся такие чрезвычайные события как землетрясение, извержение вулкана, наводнение, засуха, ураган, цунами, сель, военные действия, эпидемии, крупномасштабные забастовки и другие обстоятельства. Сторона, пострадавшая от влияния обстоятельств непреодолимой силы обязана в возможно короткий срок, но не более чем через 7 (семь) календарных дней после завершения этих обстоятельств, довести до сведения другой Стороны информацию о случившемся. Подтверждением наличия обстоятельств непреодолимой силы и их продолжительности является письменное свидетельство уполномоченных органов или уполномоченных организаций.

10.3.Банк не несет ответственности в случае, если информация о счетах и иная конфиденциальная информация о Клиенте или проведенных им банковских операций станет известна иным лицам в результате прослушивания или перехвата каналов связи во время их использования, в результате изготовления дополнительных сим-карт к телефону Клиента, либо в результате несоблюдения Клиентом условий хранения и использования информации.

10.4.Банк не несет ответственности в случае возникновения спорных ситуаций вследствие невыполнения Клиентом требований настоящих Правил, Общих правил и/или заключенных с Банком договоров.

10.5.Клиент несет ответственность за все операции, проводимые им или его представителем в соответствии с условиями Договора.

10.6.Банк не несет ответственности за технические сбои систем связи, иных технических средств и систем, повлекшие за собой неисполнение своих обязательств в соответствии с данным Договором.

10.7.В случае неисполнения или ненадлежащего исполнения своих обязательств по Договору, Банк несет ответственность только при наличии вины.

10.8.Банк не несет ответственности за невыполнение, несвоевременное или неправильное выполнение поручений Клиентов, если это было вызвано предоставлением Клиентом

недостоверной информации, потерей актуальности информации, ранее предоставленной Клиентом, недостоверной информации, используемой при регистрации и исполнении Банком поручения или вводом Клиентом ошибочных данных.

10.9.Банк не несет ответственности за ущерб, возникший вследствие несанкционированного использования третьими лицами Логина/Пароля и/или Одноразового пароля Клиента, если такое использование стало возможным не по вине Банка.

10.10.Банк не несет ответственности за ошибочную передачу Клиентом распоряжений.

10.11.Клиент несет ответственность за убытки, возникшие у Банка в результате исполнения поручений, переданных в Банк от имени Клиента неуполномоченным лицом, при условии, что это стало возможно не по вине Банка.

10.12.Клиент несет риск убытков, возникших у него в результате исполнения поручений, переданных в Банк с использованием направленных Клиенту, в установленном настоящими Правилами порядке, Одноразовых паролей.

10.13.Банк не несет ответственности, если информация об изменении/дополнении Правил и/или Тарифов, опубликованная в порядке и в сроки, установленные настоящими Правилами, не была получена и/или изучена и/или правильно истолкована Клиентом.

11.Предъявление претензий и их рассмотрение

11.1.В случае несогласия со списанием со Счета какой-либо суммы денежных средств Клиент обязан подать в Банк письменное заявление (претензию) в течение 10 (десяти) рабочих дней со дня совершения Операции. Претензия оформляется в свободной форме с изложением причин, по которым Клиент считает Операцию неправомерной, и с приложением к ней документов, подтверждающих совершение Операции списания оспариваемой суммы денежных средств.

При отсутствии обращения Клиента в Банк в срок, указанный в настоящем пункте, Операция, совершенная по Счету с использованием Системы ДБО, считается подтвержденной Клиентом.

11.2.Банк рассматривает претензию и предоставляет ответ Клиенту в течение 30 (тридцати) календарных дней со дня получения.

11.3.Банк вправе запросить у Клиента предоставление дополнительных документов и информации, необходимой для всестороннего рассмотрения претензии, в том числе документы, подтверждающие обращение Клиента в правоохранительные органы Российской Федерации.

В случае непредставления в Банк необходимых документов в течение 7 (Семи) календарных дней с момента запроса Банком у Клиента недостающих документов Банк составляет мотивированный ответ о невозможности опротестования Операции из-за недостаточности предоставленных Клиентом документов путем направления письменного уведомления Клиенту.

11.4.Если в ходе рассмотрения претензии Клиента у Банка по объективным причинам возникают сложности в расследовании обстоятельств, в том числе связанные с запросом Банком необходимых документов, то срок ее рассмотрения может быть увеличен, но не более чем на 30 (тридцать) календарных дней.

11.5.По результатам расследования Банк принимает решение о возмещении/отказе в возмещении оспариваемой суммы Операции, совершенной по Счету с использованием Системы ДБО.

11.6.В случае принятия Банком решения о возмещении Клиенту оспариваемой суммы, Банк перечисляет оспариваемую сумму Операции на Счет Клиента в течение 3 (трех) рабочих дней с даты принятия такого решения. В случае принятия Банком решения об отказе в возмещении суммы Операции Банк направляет Клиенту по Системе ДБО или иным согласованным с Клиентом способом связи, письменное уведомление с обоснованием отказа ему в возмещении денежных средств по спорной Операции.

12.Срок действия и порядок расторжения договора

12.1.Договор считается заключенным на неопределенный срок.

12.2.Договор может быть расторгнут в одностороннем порядке по инициативе любой из Сторон.

12.3.С целью расторжения Договора Клиент представляет в Банк Заявление об изменении доступа к Системе ДБО (по форме Приложения № 2 к настоящим Правилам). Договор считается расторгнутым с даты принятия заявления Банком.

12.4.При расторжении Договора по инициативе Банка, Банк направляет Клиенту письменное уведомление о расторжении Договора на адрес электронной почты Клиента, указанный Клиентом в момент заключения Договора (при его отсутствии уведомление о расторжении договора направляется почтовым отправлением на адрес регистрации Клиента, либо иной адрес, имеющийся у Банка, согласно предоставленным Клиентом сведениям). Договор считается расторгнутым с даты и времени, указанных в уведомлении, после чего прекращается прием и исполнение распоряжений Клиента.

12.5.Договор считается расторгнутым при условии отсутствия у Клиента обязательств по погашению перед Банком задолженности по Договору. При наличии указанных обязательств по погашению задолженности перед Банком Договор считается расторгнутым с момента исполнения обязанности по оплате Клиентом указанной задолженности.

12.6.Все распоряжения Клиента, зарегистрированные Банком до момента расторжения Договора, считаются поданными от имени Клиента и исполняются Банком в соответствии с условиями Договора.

12.7.Расторжение Договора не влечет прекращения обязательств по иным договорам (соглашениям), заключенным между Клиентом и Банком.

12.8.Договор прекращает свое действие при расторжении всех заключенных между Банком и Клиентом договоров текущего счета/договоров вклада/договоров текущего счета с использованием банковской карты, подключенных к Системе ДБО, в день закрытия последнего Счета.

12.9.В случае неисполнения Клиентом своих обязательств по оплате обслуживания в Системе Банк вправе произвести отключение соответствующих услуг (отключение производится Банком после 10 числа месяца, за который не внесена предусмотренная плата).

12.10.При расторжении Договора уплаченная Банку плата Клиенту не возвращается.

13.Заключительные положения

13.1.Банк извещает Клиента об изменениях Правил и (или) Тарифов за 10 (Десять) рабочих дней до даты их введения в действие путем размещения информации на информационных стендах в подразделениях Банка и на сайте Банка в сети Интернет (www.rostfinance.ru), либо иными способами, указанными в пункте 2.11. настоящих Правил по выбору Банка.

13.2.Клиент вправе согласиться с предложенными изменениями к Правилам и (или) Тарифам (акцептовать) любым из следующих способов:

- путем направления Банку письменного подтверждения согласия (акцепта) на вносимые в Правила и (или) Тарифы изменения в виде документа на бумажном носителе, подписанного собственноручно, или в виде Электронного документа с Электронной подписью либо непредставлении Банку письменного отказа в их изменении и (или) Заявления о расторжении Договора в порядке, установленном в разделе 12 настоящих Правил;
- путем предоставления с даты направления Банком предложения (оферты) Банка на изменение к Договору и (или) Тарифам Электронных документов, свидетельствующих о намерении Клиента исполнять Договор с учетом изменений.

13.3.Договор и (или) Тарифы считаются измененными по соглашению Сторон по истечении 10 (Десяти) рабочих дней после публикации сообщения (оферты) об изменениях на

сайте Банка при условии, что в течение этого срока Банк не получит от Клиента письменного Заявления о расторжении Договора.

13.4.Клиент обязан не реже 1 (Одного) раза в 5 (Пять) календарных дней знакомиться с информацией, публикуемой Банком в соответствии с пунктом 2.11. настоящих Правил.

13.5.В случае несогласия Клиента с планируемыми изменениями в Правила или Тарифы Клиент вправе расторгнуть Договор в порядке, установленном в разделе 12 настоящих Правил.

13.6.Во всем остальном, что не предусмотрено настоящими Правилами, Банк и Клиент руководствуются действующим законодательством Российской Федерации.

13.7.Все споры, возникающие между Сторонами, которые не могут быть урегулированы путем переговоров, подлежат разрешению судом в порядке, установленном законодательством Российской Федерации.

13.8.При внесении изменений и (или) дополнений в Правила, такие изменения вступают в силу и подлежат применению по истечении 10 (десяти) рабочих дней с даты размещения на Сайте, в офисе Банка текста Правил с учетом внесенных изменений. Изменения в Правила становятся обязательными для Банка и Клиента с даты введения редакции в действие. Неполучение Банком от Клиента до вступления в силу новой редакции Правил письменного уведомления о расторжении Договора считается выражением согласия Клиента на изменение настоящих Правил.

13.9.В случае изменения действующего законодательства Российской Федерации, нормативных актов Банка России или внутренних документов Банка до приведения настоящих Правил в соответствие данным изменениям настоящие Правила действуют в части им не противоречащей.

Приложение № 1. К Правилам ДБО физических лиц

В ОООКБ «РостФинанс»

ЗАЯВЛЕНИЕ
о присоединении к Правилам дистанционного банковского обслуживания физических лиц в ОООКБ «РостФинанс»

1. Ф.И.О.
клиента_____
2. Арес регистрации
Адрес места жительства
3. Тел._____ 4. ИНН _____
5. Факс_____ 6. E-mail_____

7. Документ, удостоверяющий личность _____, серия _____ номер _____,
дата выдачи «___» _____20__г., кем выдан _____
Логин в Системе ДБО (заполняется сотрудником Банка после регистрации в Системе ДБО)

_____

Кодовое слово: _____ *(для идентификации, при обращении в Банк по телефону)*

Для отправки сообщений прошу использовать (один из видов уведомления):

☐ номер телефона (SMS-информирования)
☐ номер телефона (PUSH-уведомления)

+7											

Подписанием настоящего заявления присоединяюсь к Правилам дистанционного банковского обслуживания физических лиц в ООО КБ «РостФинанс» (далее – Правила).
Даю согласие на списание Банком без дополнительных распоряжений денежных средств с моего банковского счета, открытого в Банке ООО КБ «РостФинанс», в случаях и порядке, установленных Правилами. С действующими Тарифами Банка, лимитами и ограничениями в Системе ДБО на момент подписания настоящего Заявления ознакомлен(а) и согласен(а).

_____ _____/_____/
(дата) *(подпись)* *(фамилия, имя, отчество)*

Заявление принял _____
(должность, ФИО, дата, подпись сотрудника)

Систему ДБО подключил _____
(должность, ФИО, дата, подпись сотрудника)

Приложение № 2. К Правилам ДБО физических лиц

В ОООКБ «РостФинанс»

ЗАЯВЛЕНИЕ
об изменении доступа к системе дистанционного банковского обслуживания

1. Ф.И.О.
клиента_____
2. Арес регистрации
Адрес места жительства
3. Тел._____ 4. ИНН _____
5. Факс_____ 6. E-mail_____

7. Документ, удостоверяющий личность _____, серия _____ номер
_____,
дата выдачи «___» _____20__г., кем выдан _____
Логин в Системе ДБО (заполняется сотрудником Банка после регистрации в Системе ДБО)

_____

☐ Прошу изменить контактные данные

☐ Прошу предоставить новый Логин взамен утраченного

☐ Прошу провести блокировку Системы ДБО

☐ Прошу восстановить доступ к Системе ДБО

☐ Прошу расторгнуть Договор о предоставлении банковских услуг физическим лицам с использованием системы дистанционного банковского обслуживания

Для отправки сообщений прошу использовать (один из видов уведомления):

☐ номер телефона (SMS-информирования)

☐ номер телефона (PUSH-уведомления)

+7											

_____ _____/_____/

(дата) *(подпись)* *(фамилия, имя, отчество)*

Заявление принял _____
(должность, ФИО, дата, подпись сотрудника)

Систему ДБО подключил _____
(должность, ФИО, дата, подпись сотрудника)

Лимиты на осуществление банковских операций физическими лицами в Системе ДБО

<table>
<tr><th rowspan="2">№ п/п</th><th rowspan="2">Наименование операции</th><th colspan="3">Размер Лимита</th></tr>
<tr><th>В месяц, руб.</th><th>В день, руб.</th><th>Одной операции, руб.</th></tr>
<tr><td>1.1.</td><td>Внутрибанковские переводы между своими счетами в валюте Российской Федерации. Переводы платежей в бюджет и во внебюджетные фонды Российской Федерации</td><td rowspan="5">-</td><td rowspan="5">400 000</td><td>Без ограничений</td></tr>
<tr><td>1.2.</td><td>Переводы в валюте Российской Федерации на счета других клиентов – физических[1] и юридических лиц, открытые в Банке и в других кредитных организациях, в т.ч. в режиме «Оплата услуг» (за исключением п.1.3 и 1.5.)</td><td>100 000</td></tr>
<tr><td rowspan="3">1.3.</td><td>Платежи в адрес получателей: Билайн, Мегафон, МТС, Теле 2, иных операторов сотовой связи;</td><td rowspan="3">15 000</td></tr>
<tr><td>Яндекс.Деньги, QIWI, RAPIDA, WebMoney, оплата любых электронных кошельков</td></tr>
<tr><td>Перевод денежных средств с банковской карты Банка на банковскую карту любого российского банка (услуга «Card2Card») [2]</td></tr>
<tr><td>1.4.</td><td>Внутрибанковские переводы на свои счета (в случае, если счет списания и счет зачисления открыты в разных валютах (безналичная конверсия))[3]</td><td rowspan="2">400 000</td><td rowspan="2">-</td><td rowspan="2">-</td></tr>
<tr><td>1.5.</td><td>Переводы в валюте Российской Федерации на счета других клиентов – физических в других кредитных организациях с использованием системы быстрых платежей платежной системы Банка России (СБП)</td></tr>
<tr><td colspan="5">[1] Переводы на счета Банковских карт осуществляются при условии указания лицевого счета Банковской карты и реквизитов Банка – эмитента.</td></tr>
<tr><td colspan="5">[2] Переводы осуществляются при условии указания номера Банковской карты физического лица – получателя перевода.</td></tr>
<tr><td colspan="5">[3] Услуга предоставляется с понедельника по пятницу с 9 часов 00 минут до 16 часов 00 минут МСК</td></tr>
</table>

ПАМЯТКА
О мерах по безопасному использованию электронного средства платежа

Уважаемые клиенты!

Настоящая Памятка направлена на информирование ООО КБ «РостФинанс» своих Клиентов в соответствии с рекомендациями Банка России в рамках реализации комплекса мер по повышению финансовой грамотности населения и на основе анализа практики использованию физическими и юридическими лицами электронного средства платежа. Соблюдение рекомендаций, содержащихся в настоящей Памятке, позволит Вам предупредить несанкционированные операции с использованием электронных средств и способов платежа при:

- Проведении операций с банковской картой в банкомате;
- Безналичной оплате банковской картой товаров и услуг, в том числе за рубежом;
- Оплате банковской картой в сети Интернет;
- Использовании систем ДБО.

1. Основные понятия

Банк – ООО КБ «РостФинанс».

Банковская карта – персональная расчетная карта платежной системы, являющаяся электронным средством платежа.

ДБО – Система дистанционного банковского обслуживания.

Ключ ЭП – уникальная последовательность символов, предназначенная для создания электронной подписи.

Открытый ключ ЭП – уникальная последовательность символов,
соответствующая Закрытому ключу ЭП, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной подписи подлинности ЭП в электронном документе.

Закрытый ключ ЭП – уникальная последовательность символов, известная Владельцу ЭП и предназначенная для создания в электронном документе электронной подписи.

Пара ключей ЭП Клиента – Закрытый ключ ЭП Клиента и соответствующих ему открытый ключ ЭП Клиента.

Ключевой носитель (Внешний отчуждаемый носитель закрытого ключа ЭП с криптографическими возможностями) – персональное средство строгой аутентификации и хранения данных (eToken, ruToken ГОСТ), аппаратно поддерживающее работу с Закрытым ключом ЭП, позволяющее осуществлять механизм электронной подписи так, что Закрытый ключ ЭП никогда не покидает пределы носителя, что исключает возможность компрометации ключа (за исключением утраты и хищения) и повышает общую безопасность системы ДБО.

Система ДБО – система дистанционного банковского обслуживания, обмена электронными документами, включающая комплекс программно-аппаратных средств и организационных мероприятий для составления, удостоверения, передачи и обработки ЭД по телекоммуникационным каналам связи, используемым Клиентом и Банком. Банк предоставляет своим Клиентам дистанционное банковское обслуживание с использованием
Интернет-банка и/или Мобильного банка:
Интернет-банк – сервис ДБО, позволяющий управлять банковскими счетами в рублях и иностранной валюте, а также управлять другими банковскими продуктами в режиме реального времени посредством сети Интернет.
Мобильный банк – сервис ДБО, мобильное приложение, предоставляющее Клиенту возможность доступа к Интернет-банку, с использованием мобильного устройства
на базе операционной системы iOS или Android.

Срок действия ЭП – период времени, по истечении которого ЭП является недействительной.

Средство подтверждения/Одноразовый пароль – средство подтверждения Клиентом неизменности, подлинности и целостности передаваемого по системе ДБО распоряжения. Формируется системой ДБО и направляется Клиенту (Представителю клиента) на указанный им номер мобильного телефона посредством sms-сообщения/ Push-уведомления для удостоверения права распоряжения средствами на счетах при совершении операций, является простой ЭП Клиента в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Электронное средство платежа (ЭСП) **–** средство и (или) способ, позволяющие Клиенту Банка составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий (ИКТ), электронных носителей информации, в том числе платежных карт, а также иных технических устройств, как пример ЭСП: платежные карты, USB-устройства «eToken», ruToken ГОСТ, система ДБО, электронные кошельки WebMoney и Яндекс.Деньги и др.

Электронная подпись (ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией. ЭП предназначена для защиты электронного документа от подделки и идентификации Владельца ЭП, установления отсутствия искажения информации в электронном документе.

CVV2/CVC2 (англ. Card Verification Value 2) – трехзначный или четырехзначный цифровой код на обратной стороне карты (в конце панели образца подписи), который используется Клиентом конфиденциально как способ удостоверения распоряжений по операциям с реквизитами карты в сети Интернет.

IP-адрес – это уникальный идентификатор (адрес) устройства (обычно компьютера), подключенного к локальной сети или Интернету. Назначается при подключении устройства к локальной сети или Интернету.

IP/MAC-фильтрация – ограничение подключения к системе ДБО по определенному IP-адресу или MAC-адресу.

MAC-адрес – это уникальный идентификатор, присваиваемый изготовителем каждой единице оборудования компьютерных сетей, используемый для идентификации рабочего места.

SMS Security – комплекс средств обеспечения безопасности, предназначенный для дополнительной аутентификации Клиента в системе ДБО по одноразовым паролям.

SMS-информирование/Push-уведомления – это возможность контролировать состояние счета с помощью мобильного телефона. Сервис «SMS-информирование» / «Push-уведомления», предоставляется в рамках услуги обслуживания счетов с использованием системы ДБО, с использованием банковской карты и (или) ее реквизитов. Данный сервис предназначен для повышения качества обслуживания Ваших банковских счетов и безопасности проведения операций с использованием систем ДБО, а также банковских карт.

2.Общие рекомендации

Запрещается:

– сообщать ПИН-код, данные Вашей банковской карты и пароль для входа в систему ДБО третьим лицам, в том числе родственникам, знакомым, сотрудникам Банка, кассирам и лицам, помогающим Вам в использовании ЭСП;

– передавать ЭСП для использования третьим лицам, в том числе родственникам. Если на ЭСП нанесены фамилия и имя физического лица, то только это физическое лицо имеет право использовать ЭСП;

– отвечать на электронные письма/ телефонные звонки/ SMS-сообщения, в которых от имени Банка предлагается предоставить данные ЭСП. Не

рекомендуется переходить по «ссылкам», указанным в электронных письмах (включая ссылки на сайт Банка), т.к. такие ссылки могут вести на сайты-двойники.

Рекомендуется:

– запомнить ПИН-код или в случае, если это является затруднительным, хранить его отдельно от банковской карты в неявном виде и недоступном для третьих лиц, в том числе родственников, месте;

– запомнить пароль для входа в систему ДБО, после завершения сеанса работы в системе ДБО хранить ключевой носитель в недоступном для третьих лиц месте;
– при получении банковской карты расписаться на ее оборотной стороне в месте, предназначенном для подписи держателя банковской карты, если это предусмотрено. Это снизит риск использования ее без Вашего согласия в случае ее утраты;

– уделять особое внимание условиям хранения и использования банковской карты. Не подвергать банковскую карту механическим, температурным и электромагнитным воздействиям, а также избегать попадания на нее влаги. Банковскую карту не рекомендуется хранить рядом с мобильным телефоном, бытовой и офисной техникой;

– всегда иметь при себе контактные телефоны Банка. Телефон Банка, осуществившего выпуск платежной карты, указан на оборотной стороне банковской карты;

– с целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковской карты установить суточный лимит на сумму операций по банковской карте и одновременно подключить электронную услугу оповещения о проведенных операциях (например, оповещение посредством SMS-сообщений или иным способом);

– в целях информационного взаимодействия с Банком использовать только реквизиты средств связи (мобильных и стационарных телефонов, факсов, интерактивных web-сайтов/порталов, обычной и электронной почты и пр.), которые указаны в документах, полученных непосредственно в Банке;

– помнить, что в случае раскрытия ПИН-кода, персональных данных, утраты банковской карты существует риск совершения неправомерных действий с использованием принадлежащей Вам банковской карты со стороны третьих лиц. Если имеются предположения о раскрытии ПИН-кода, персональных данных, позволяющих совершить неправомерные действия с Вашим банковским счетом, а также если банковская карта была утрачена, необходимо немедленно обратиться в Банк для блокировки банковской карты и следовать указаниям сотрудника Банка. До момента обращения в Банк Вы несете риск, связанный с несанкционированным списанием денежных средств с Вашего банковского счета;

– установить на свой компьютер, мобильное устройство антивирусное программное обеспечение и регулярно проводить его обновление и обновление других используемых Вами программных продуктов (операционной системы и прикладных программ), это может защитить Вас от проникновения вредоносного программного обеспечения и снизит риски несанкционированного использования систем ДБО и банковской карты для оплаты в сети Интернет;

– незамедлительно проводить замену сертификата проверки ключа ЭП при смене должностных лиц, наделенных полномочиями по распоряжению денежными средствами на расчетном счете юридического лица.

3.Рекомендации при совершении операций с банковской картой в банкомате

Осуществляйте операции с использованием банкоматов, установленных в безопасных местах (например, в государственных учреждениях, подразделениях банков, крупных торговых комплексах, гостиницах, аэропортах и т.п.).

Не используйте устройства, считывающие магнитную полосу банковской карты, которые требуют ввода ПИН-кода для доступа в помещение, где расположен банкомат, и другие внешние устройства, которые считывают магнитную полосу карты.

Перед использованием банкомата осмотрите его на наличие дополнительных устройств, не соответствующих его конструкции и расположенных в месте набора ПИН-кода и в месте (прорезь), предназначенном для приема банковских карт (например, наличие неровно установленной клавиатуры набора ПИН-кода). При появлении подозрений о наличии дополнительных устройств на банкомате воздержитесь от использования такого банкомата и сообщите о своих подозрениях сотрудникам Банка по телефону, указанному на банкомате.

Не применяйте физическую силу, чтобы вставить банковскую карту в банкомат. Если банковская карта не вставляется, воздержитесь от использования такого банкомата, возможно, он сломан или подвергся мошенническим действиям.

Набирайте ПИН-код банковской карты таким образом, чтобы люди, находящиеся в непосредственной близости, не смогли его увидеть. При наборе ПИН-кода прикрывайте клавиатуру рукой. Применение данных мер защитит от подсматривания Вашего ПИН-кода как посторонними людьми, так и при наличии на банкомате несанкционированно установленного видеоустройства с целью осуществления мошеннических действий.

В случае если банкомат работает некорректно (например, долгое время находится в режиме ожидания, самопроизвольно перезагружается), следует отказаться от использования такого банкомата, отменить текущую операцию, нажав на клавиатуре кнопку «Отмена», и дождаться возврата банковской карты.

После получения наличных денежных средств в банкомате следует пересчитать банкноты полистно, убедиться в том, что банковская карта была возвращена банкоматом, дождаться выдачи квитанции при ее запросе, затем положить их в сумку (кошелек, карман) и только после этого отходить от банкомата.

Следует сохранять распечатанные банкоматом квитанции для последующей сверки указанных в них сумм с выпиской по банковскому счету.

Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций с банковской картой в банкоматах, тем более не давайте им в руки свою банковскую карту.

Если при проведении операций с банковской картой в банкомате банкомат не возвращает банковскую карту, следует позвонить по телефону, указанному на банкомате, и объяснить обстоятельства произошедшего, а также следует обратиться в банк, выдавший банковскую карту, которая не была возвращена банкоматом, и в обязательном порядке заблокировать банковскую карту, следуя инструкциям сотрудника банка.

При приеме и возврате карты устройством самообслуживания не толкайте и не выдергивайте карту до окончания ее прерывистого движения в картоприемнике.

Неравномерное движение карты не является сбоем, а необходимо для защиты Вашей карты от компрометации.

В случаях возникновения подозрения о нарушении порядка штатного функционирования банкомата, а также в случаях выявления признаков событий, связанных с нарушением обеспечения защиты информации при осуществлении переводов денежных средств с применением банкомата, действуйте в соответствии с информацией, размещенной на банкомате.

4.Рекомендации при безналичной оплате банковской картой товаров и услуг

Не используйте банковские карты в организациях торговли и услуг, не вызывающих доверия.

Требуйте проведения операций с банковской картой только в Вашем присутствии. Это необходимо в целях снижения риска неправомерного получения Ваших персональных данных и платежных данных банковской карты, указанных на самой карте.

При проведении операции с вашей банковской картой не упускайте ее из виду.

Не допускайте ситуаций, когда банковская карта находится вне Вашего поля зрения (например, загораживается монитором кассы).

Рекомендуется защищать от подсматривания данные банковской карты, находящиеся на ее обратной стороне. Верчение карты, также как и поворачивание карты обратной стороной в людном месте может снизить конфиденциальность платежных данных, указанных на банковской карте.

При использовании банковской карты для оплаты товаров и услуг кассир может потребовать от владельца банковской карты предоставить паспорт, подписать чек или ввести ПИН-код. Перед набором ПИН-кода следует убедиться в том, что люди, находящиеся в непосредственной близости, не смогут его увидеть. Перед тем как подписать чек, в обязательном порядке проверьте сумму, указанную на чеке.

По завершении операции кассир должен выдать Вам кассовый чек или торговый слип. Не подписывайте чек (слип), в котором не проставлены (не соответствуют действительности) сумма, валюта, дата операции, тип операции, название торгово-сервисной точки.

В случае если при попытке оплаты банковской картой имела место «неуспешная» операция, следует потребовать у кассира и сохранить один экземпляр выданного терминалом чека (слипа) для последующей проверки на отсутствие указанной операции в выписке по банковскому счету.

В случае Вашего отказа от покупки сразу же после завершения операции, требуйте отмены операции и убедитесь в том, что торгово-сервисным предприятием уничтожен ранее оформленный чек (слип).

Сохраняйте все чеки (слипы) в течение длительного времени. Не выбрасывайте слипы и чеки, на которых отображен полный номер карт.

5.Рекомендации при совершении операций с банковской картой через сеть Интернет

Не используйте ПИН-код при заказе товаров и услуг через сеть Интернет, а также по телефону/факсу.

Не сообщайте персональные данные или информацию о банковской карте или банковском счете по открытым каналам через сеть Интернет, например, ПИН-код, пароли доступа к ресурсам Банка, срок действия банковской карты, кредитные лимиты, историю операций, персональные данные.

С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковского счета рекомендуется для оплаты покупок в сети

Интернет использовать отдельную банковскую карту (так называемую виртуальную карту) с предельным лимитом, предназначенную только для указанной цели и не позволяющую проводить с ее использованием операции в организациях торговли и услуг.

Следует пользоваться интернет-сайтами только известных и проверенных организаций торговли и услуг.

Обязательно убедитесь в правильности адресов интернет-сайтов, к которым подключаетесь и на которых собираетесь совершить покупки, т.к. похожие адреса могут использоваться для осуществления неправомерных действий.

Убедитесь, что интернет-сайт содержит справочную информацию об интернет магазине, которая включает в себя: наименование юридического лица или индивидуального предпринимателя, юридический и фактический адреса, контактный номер телефона и адрес электронной почты для обращения покупателей.

Рекомендуется совершать покупки только со своего компьютера в целях сохранения конфиденциальности персональных данных и информации о банковской карте или банковском счете. В случае, если покупка совершается с использованием чужого компьютера, не рекомендуется сохранять на нем персональные данные и другую информацию, а после завершения всех операций нужно убедиться, что персональные данные и другая информация не сохранились (вновь загрузив в браузере интернет-страницу продавца, на которой совершались покупки)

6.Рекомендации по процедуре опротестования операций, совершенных клиентами – физическими лицами с использованием платежных карт в торгово-сервисных предприятиях, находящихся за пределами Российской Федерации

Необходимо внимательно ознакомиться с условиями договора с ТСП до момента оплаты товаров (услуг), заранее оценив риски утраты денежных средств. Защита гражданами Российской Федерации своих прав в случае недобросовестности иностранных ТСП может быть затруднительной вследствие необходимости применения норм иностранного законодательства.

В момент оплаты сохранять все документы/чеки/квитанции.

Взаимодействовать с ТСП в соответствии с договором, в том числе в случаях, когда ТСП не была оказана либо некачественно оказана оплаченная с использованием платежной карты услуга, не была осуществлена поставка оплаченного товара.

В случае противоправных действий со стороны третьих лиц под видом иностранного ТСП необходимо обратиться с соответствующим заявлением в правоохранительные органы.

Взаимодействие с Банком осуществляется в соответствии с Договором текущего счета с использованием банковской карты (для физических лиц).

Условия опротестования операций с использованием платежных карт в соответствии с правилами карточных платежных систем:

о своих претензиях по операциям Клиент сообщает Банку в течение 30 (тридцати) календарных дней со дня списания суммы операции со Счета карты путем оформления заявления в офисе Банка;

срок рассмотрения Заявления не превышает 30 (тридцать) дней, а в случае осуществления трансграничного перевода денежных средств – 60 (шестьдесят) дней со дня его получения

7.Рекомендации при использовании системы ДБО

Ключевая информация – это аналог Вашей личной подписи и ответственность за ее сохранение ложится на пользователя системы ДБО. Помните, что наличие ключа ЭП позволяет заверить от Вашего имени документ и передать его на исполнение в Банк.

При использовании ключа ЭП соблюдайте следующие правила:

-Подключите услугу «SMS-Информирование»/Push-уведомления, с помощью которой Банк будет оперативно информировать о списаниях с банковского счета. Получите ключевой носитель в Банке лично, а не через доверенных лиц.

-Не передавайте ключевой носитель третьим лицам, не оставляйте его без присмотра, не храните в доступном месте.

-При получении ключевого носителя создайте резервную копию, хранимую в сейфе (кроме хранения ключей на eToken).

-На электронном носителе, на котором расположены ключи, не должно быть другой информации.

-Хранение ключа ЭП на жестком диске недопустимо.

-Вставляйте ключевой носитель только на время работы в системе ДБО.

-Не допускайте к работе с компьютером, на котором установлена система ДБО, посторонних лиц (неуполномоченных для работы с ключами ЭП). Периодически меняйте пароль для входа в систему ДБО (оптимальный срок действия пароля 2-3 месяца).

-Не создавайте слишком простых паролей (например: 111111, 12345, abcdefg, qwerty и т.п.) – не используйте в качестве пароля дату рождения, номер телефона и другие данные, которые можно легко узнать.

-Постоянно контролируйте состояние счета путем просмотра выписки (рекомендуется проверять состояние счета не реже одного раза в день).

-Обращайте внимание на дату и время последних входов в систему.

Клиентом могут быть использованы дополнительные средства обеспечения безопасности:

-SMS Security – услуга Банка по передаче одноразового пароля, используемого для дополнительной аутентификации при входе в систему ДБО, а также для дополнительного подтверждения подписываемых документов, которая предоставляется Клиенту Банком посредством SMS-сообщений/ Push-уведомления (коротких текстовых сообщений) на номер мобильного (сотового) телефона Клиента.

При возможности необходимо:

-отказаться от использования ключей ЭП на незащищенных носителях – дискетах, USB- и прочих носителях. Для хранения ключей ЭП пользуйтесь защищенными носителями eToken, ruToken ГОСТ;

-установить верхний лимит суммы платежа, проводимого через систему ДБО, для чего следует обратиться в Банк;

-установить перечень возможных получателей денежных средств, в адрес которых могут быть совершены переводы денежных средств с использованием системы ДБО;

-установить временной период, в который могут быть совершены переводы денежных средств с использованием системы ДБО;

-внедрить использование для отправки документов двух ЭП, хранимых на разных носителях (украсть два ключа сложнее, чем один);

-согласовать с Банком включение функции фильтрации по IP-адресам и/или MAC-адресу сетевой карты (IP/MAC-адреса). В этом случае работа в системе будет возможна только с того компьютера, IP/MAC-адрес которого был указан при включении функции фильтрации.

При компрометации (утрата, в том числе с последующим обнаружением, хищение, разглашение, несанкционированное копирование, передача по любым каналам связи, и т.д.) или попытке компрометации ключей ЭП или компьютера/мобильного устройства, увольнения ответственного сотрудника или ИТ-специалиста Вашей компании, который имел доступ, даже потенциально, к компьютеру/мобильному устройству или к ключам ЭП, необходимо незамедлительно:

-прекратить использование системы ДБО,

-обратиться в Банк для блокировки ключей ЭП и генерации новых.

При работе в системе ДБО адрес сайта должен начинаться:

https://business.faktura.ru/f2b/?site=rostfinance

https://elf.faktura.ru/elf/app/?site=rostfinance

Особое внимание уделяйте наличию https в начале адреса, который свидетельствует о работе в системе ДБО Банка по защищенному соединению с шифрованием всех передаваемых данных.

Незамедлительно сообщайте в Банк о факте невозможности получения доступа к системе ДБО, по причине несовпадения пароля для входа в систему. Обычной практикой злоумышленников является смена пароля для маскирования своих действий и получения дополнительного времени для успешного выполнения операций от имени Клиента.

В случае невыясненных сбоев в работе компьютера/мобильного устройства Клиента, на котором установлена система ДБО, рекомендуется немедленно отключить компьютер/мобильное устройство. Произвести по телефону сверку остатков на счете с Банком, при установлении несанкционированных платежей произвести их отзыв.

Компьютер/мобильное устройство в целях сохранения данных, до начала работы экспертной комиссии, опечатать и не включать.

Персональные компьютеры, на которых ведется работа в системе ДБО, должны отвечать следующим требованиям:

-На компьютере должна быть установлена и своевременно обновляться лицензионная операционная система Windows XP SP3, 7, 8, 10 или с операционной системой

- OS X 10.10 и выше или mac OS 10.12 и выше и лицензионное антивирусное программное обеспечение (далее – ПО) с актуальными антивирусными базами (AVP Kaspersky, Symantec AntiVirus, NOD32 и т.д.).

-Антивирусное ПО должно быть запущено постоянно с момента загрузки компьютера. Рекомендуется полная еженедельная проверка компьютера на наличие вирусов, удаление обнаруженного вредоносного ПО.

-Должен быть настроен персональный межсетевой экран (брандмауэр, фаервол).

-Пароли учетных записей, обладающих правами администратора, должны быть сложными.

-Учетная запись «Гость» должна быть выключена.

-Не должно быть учетных записей с пустыми паролями.

-Рекомендуется не использовать права администратора при отсутствии необходимости. В повседневной практике рекомендуется входить в систему как пользователь, не имеющий прав администратора.

-Должен быть включен системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ. Необходимо периодически просматривать журнал аудита событий и реагировать на ошибки.

-Необходимо своевременно обновлять операционную систему (установка патчей, критичных обновлений).

-Контроль учетных записей (UAC) не должен быть отключен. UAC используется для предотвращения несанкционированных изменений на компьютере.

В случаях, наличия у Банка признаков несанкционированных платежей или признаков рисковых операций по счетам Клиентов Банка, ответственный сотрудник Банка либо ответственный сотрудник Фактура.ру, Золотая Корона (далее – служба мониторинга, служба проверки операций) связывается по телефону с Клиентом, указанному в официальных документах, представленных Клиентом в Банк для предотвращения и выявления мошеннических атак.

-В этих случаях происходит идентификация Клиента – может запрашиваться ФИО отправителя (создателя платежа), паспортные данные отправителя платежа, дата рождения, наименование отправителя платежа, адрес регистрации юридического лица, реквизиты платежа и т.п.

-Для обращения к Клиентам с этой целью используются официальные телефоны Банка +8 800 7777 001.

-При этом, никакие ПИН-коды, логины/пароли, кодовые слова, иные идентификаторы, позволяющие осуществить платеж по счету Клиента без его согласия, сотрудниками Банка и

(или) службы мониторинга не запрашиваются и со стороны Клиента не должны быть представлены.

В целях предотвращения несанкционированного доступа к защищаемой информации при утрате (потере, хищении) устройства, с использованием которого Клиентом осуществлялся перевод денежных средств, необходимо обратиться в службу поддержки системы и заблокировать возможность переводов до выяснения обстоятельств.

Клиенту рекомендуется устанавливать на устройство, с использованием которого осуществляется перевод денежных средств, программные средства, позволяющие контролировать конфигурацию устройства (в т.ч. обнаружения внесения несанкционированных изменений в установленное ПО).

В случае установки на компьютеры, на которых ведется работа в системе ДБО, программ для удаленной поддержки пользователей (например, TeamViewer, AnyDesk и т.п.),

Клиент полностью принимает на себя все риски настроек безопасности доступа в этих программах, передачи третьим лицам (в т.ч. сотрудникам Банка) идентификаторов своих рабочих мест и принятия согласия на подключение третьих лиц (в т.ч. сотрудников Банка) к своим рабочим места.

Круглосуточная служба поддержки держателей карт 8 800 7777 001
Служба поддержки системы ДБО 8 800 7777 001