ПОРЯДОК ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА

(расчетной (дебетовой) карты, кредитной карты, ДБО)

Действует с 23.10.2013 г.

в ред. от 12.10.2017, 25.01.2019

1. Термины и определения

1.1. Электронное средство платежа - 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, электронных носителей информации, в том числе платежных карт (далее банковских карт), а также иных технических устройств.

1.2. Несанкционированная операция – операция, совершенная с использованием электронных средств платежа, без согласия Клиента (совершенная неуполномоченными лицами, в том числе в результате противоправных действий) и признанная таковой Банком или судом.

1.3. Электронное средство платежа банка - банковская карта систем «Золотая Корона» /MasterCard/VISA/МИР, системы ДБО (в том числе интернет-банк «КББ-ОНЛАЙН»/мобильное приложение «КББ-ОНЛАЙН), Инфосервис.

1.4. Ключевая информация – открытые, закрытые ключи подписи, цифровые сертификаты, иная информация в электронном виде, переданная Банком Клиенту в целях дистанционного банковского обслуживания (ДБО).

1.5. Парольная информация – пароли, кодовые слова, иная информация, переданная Банком Клиенту в целях ДБО.

1.6. Компрометация ключевой информации – утрата, хищение, несанкционированное копирование, передача ключевой информации в линию связи в открытом виде, любые другие виды разглашения содержания ключевой информации, а также случаи, когда нельзя достоверно установить, что произошло с носителями, содержащими ключевую информацию (в том числе случаи, когда носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате действий злоумышленника).

1.7. Компрометация парольной информации – утрата, хищение, передача парольной информации третьим лицам.

1.8. CVV2/CVC2 - CVV2 (Card Verification Value) для карт Visa или CVC2 (Card Verification Code) для карт MasterCard или ППК2 (Проверочный параметр карты 2) для карт МИР - специальное число, состоящее из трех цифр, обеспечивающее дополнительную безопасность при таких транзакциях, при которых сама карта не присутствует, а используются её реквизиты.

2. **Информирование.**

2.1. В целях исполнения требований законодательства и обеспечения безопасности денежных средств Клиента, в соответствии с имеющейся у Банка контактной информации Клиента, полученной от Клиента при выдаче/подключении электронного средства платежа, Банк осуществляет уведомление о совершении каждой операции с использованием электронного средства платежа, после ее проведения.

2.1.1. Информирование об операциях производится в порядке и способом, указанным Клиентом в заявлении. Об операциях о переводе денежных средств с использованием карты уведомление может осуществляться:

- на номер мобильного телефона – в формате sms/push-сообщения;
- на e-mail – информирование по каждой операции, после проведения операции по счету или выпиской;
- выпиской на бумажном носителе при личном обращении в банк Клиента.

2.1.2. Об операциях о переводе денежных средств с использованием системы ДБО уведомление может осуществляться:

- на номер мобильного телефона – в формате sms/push сообщений;
- на e-mail – информирование о каждой операции, после проведения операции по счету.

2.1.3. Клиент может обратиться в Банк для изменения способа информирования, указанного в заявлении, в течение срока действия электронного средства платежа. Перечень услуг информирования размещен на web-сайте банка: http://www.kbb.ru/services/252/6219/.

2.1.4. Аутентификация клиента и подтверждение права доступа к системе ДБО, при формировании распоряжения о переводе денежных средств, включая сумму и получателя денежных средств, до

подтверждения клиентом указанного распоряжения осуществляется с использованием одноразового кода подтверждения на номер мобильного телефона в формате sms/push сообщения.

О входе в систему ДБО информирование осуществляется:

- на номер мобильного телефона – в формате sms/push сообщений;
- на e-mail – электронным письмом.

2.2. Клиент обязан:

2.2.1. предоставить Банку в письменной форме следующую контактную информацию:

2.2.1.1. действительный номер мобильного телефона российского оператора;

2.2.1.2. адрес электронной почты (E-mail);

2.2.2. обеспечить постоянную доступность номера мобильного телефона/адрес электронной почты и ежедневно проверять SMS/PUSH-сообщения/сообщения электронной почты.

2.2.3. в случае замены либо утраты номера мобильного телефона / адреса электронной почты, незамедлительно уведомить об этом Банк в письменной форме;

2.2.4. в случае утраты мобильного телефона, незамедлительно заблокировать SIM-карту;

2.2.5. ежедневно в системах ДБО (в том числе интернет-банк «КББ-ОНЛАЙН»/мобильное приложение «КББ-ОНЛАЙН) проверять состояние всех своих счетов, включая остаток по счету, доступный баланс по счету, операции по счету, заблокированные (зарезервированные) суммы операций, и незамедлительно уведомлять Банк лично о наличии ошибок, неточностей или возникновении вопросов в отношении информации, содержащейся в системах ДБО.

2.3. Клиент уведомлен, что дата и время проведения операций по счету, подтверждающих совершение операций по банковской карте, отличается от даты и времени совершения операции.

2.4. Клиент несет ответственность за подлинность номера мобильного телефона/ адреса электронной почты, а также их состояние и сохранность.

2.5. При направлении Банком сообщения на номер мобильного телефона/адрес электронной почты в соответствии с имеющейся у Банка контактной информацией Клиента обязанность Банка по информированию считается исполненной в дату и время отправления сообщения. Банк не несет ответственности за недоставку сообщения, в случае если это обусловлено причинами, не зависящими от Банка.

2.6. Предоставленные Клиентом номер мобильного телефона, адрес электронной почты, внесенные Банком в свои информационные системы, используются Банком в целях уведомления Клиента, для обеспечения безопасности операций Клиента, в том числе при компрометации электронного средства платежа/ключевой, парольной информации.

2.7. При отказе Клиента в предоставлении контактной информации, от получения уведомлений Банка, Клиент принимает все риски и единолично несет ответственность, при несанкционированном использовании электронного средства платежа.

2.8. При нарушении Клиентом Порядка использования электронного средства платежа, компрометации ключевой/парольной информации, отсутствия действительного и подлинного номера мобильного телефона/адреса электронной почты доступ Клиента ко всем функциям электронного средства платежа не предоставляется либо приостанавливается Банком. Приостановление или прекращение права клиента использовать электронное средство платежа, не прекращает действия договора банковского счета.

3. Общие меры безопасности

3.1. Для безопасного использования электронного средства платежа Клиент обязан выполнять следующие требования:

3.1.1. при получении сообщения в формате SMS/PUSH, либо в электронном формате по электронной почте, либо звонка по телефону Клиент обязан убедиться, что такое сообщение/звонок исходит именно от Банка или уполномоченного им лица;

3.1.2. не допускать компрометации ключевой и парольной информации;

3.1.3. соблюдать рекомендации по обеспечению безопасности, размещенные на следующих ресурсах в сети Интернет: на сайте Банка, на сайтах производителей соответствующих систем ДБО, на сайтах соответствующих платежных систем.

3.1.4. В случае выявления Клиентом ситуации или возникновения подозрения у Клиента, что по его счету была совершена несанкционированная операция с использованием электронного средства платежа, Клиент обязан на момент выявления или возникновения такого подозрения предпринять все меры по обеспечению:

3.1.4.1. сохранности электронных средств платежа, компьютеров либо иных электронных устройств, используемых в работе с системами ДБО, компьютерных программ и операционных систем, установленных на устройствах;

3.1.4.2. неизменности состояния счета.

3.2. В случае получения Клиентом следующих сообщений:

3.2.1.1. сообщение поступило не от Банка или уполномоченного им лица, или

3.2.1.2. сообщение поступило не с официальных телефонных номеров Банка, которые указаны на официальном сайте Банка в сети Интернет, или
3.2.1.3. запрашиваемые в сообщении действия требуют срочного ответа Клиента, или
3.2.1.4. сообщение требует предоставить, обновить или подтвердить персональную информацию Клиента, (например, девичью фамилию матери, кодовое слово, ПИН-код, номер телефона, реквизиты банковской карты, имя пользователя, пароль, иную ключевую/парольную информацию), или
3.2.1.5. сообщение содержит форму для ввода персональной информации Клиента, или
3.2.1.6. в сообщении содержится информация, что на счёт Клиента непредвиденно для него поступили денежные средства, или
3.2.1.7. в сообщении содержится просьба войти в систему ДБО по указанной ссылке, или
3.2.1.8. полученная информация вызывает любые сомнения или подозрение на мошенничество.
Клиенту следует отказаться от выполнения действий, изложенных в сообщениях, так как они не являются безопасными. Также Клиенту необходимо прекратить использование электронных средств платежа, систем ДБО и незамедлительно связаться с Банком по официальным телефонам, через службу обратной связи на сайте банка в сети Интернет либо другим способом.
3.3. В случае утраты/кражи электронного средства платежа, ключевой/парольной информации, Клиент незамедлительно обязан сообщить об этом по телефонам, указанным на web-сайте Банка либо в Памятке держателя, и следовать полученным инструкциям для блокировки/внесения в черный список электронного средства платежа или лично представить непосредственно в Банк соответствующее письменное уведомление по форме Банка. Любое устное обращение должно быть подтверждено письменным заявлением держателя в банк в течение трех календарных дней с даты устного сообщения.
В случае обнаружения факта использования без согласия Клиента электронного средства платежа, Клиент обязан лично представить непосредственно в Банк соответствующее письменное заявление по форме Банка, не позднее дня, следующего за днем направления Банком сообщения о совершенной несанкционированной операции.

4. Правила безопасности – системы ДБО через сеть Интернет (в том числе интернет-банк «КББ-ОНЛАЙН»/мобильное приложение «КББ-ОНЛАЙН).

4.1. При использовании систем ДБО Клиент обязан:
4.1.1. убедиться в безопасности компьютера (или иного устройства), с которого осуществляется доступ к сети Интернет, в том числе:
4.1.1.1. используется лицензионное программное обеспечение,
4.1.1.2. отсутствуют вирусы, вредоносные и шпионские программы,
4.1.1.3. исключен несанкционированный доступ к компьютеру из сети Интернет или локальной сети.
4.1.2. не использовать систему ДБО, если:
4.1.2.1. сайт системы ДБО в сети Интернет не является подлинным официальным сайтом системы ДБО;
4.1.2.2. соединение с сайтом системы ДБО не зашифровано (отсутствует индикация работы браузера в защищенном режиме) или при его посещении возникают ошибки проверки подлинности сертификата;
4.1.2.3. Клиент самостоятельно не указывал адрес сайта системы ДБО в соответствующем поле браузера или доступ на сайт был осуществлен по какой-либо ссылке;
4.1.2.4. компьютер/устройство, с которого осуществляется доступ к сети Интернет, может содержать вирусы, вредоносные или шпионские программы;
4.1.2.5. возможен несанкционированный доступ к компьютеру/устройству из сети Интернет или локальной сети;
4.1.2.6. запрашивается ПИН-код.
4.1.3. регулярно менять пароль для доступа в системы ДБО, при этом пароль должен быть сложным для подбора и не повторяться;
4.1.4. не входить в системы ДБО с использованием компьютера общего пользования или в местах, в которых доступ к сети Интернет является общим, а также в присутствии посторонних лиц;
4.1.5. при входе в системы ДБО:
4.1.5.1. проверять дату и время последнего входа в системы ДБО. В случае подозрения на несанкционированный доступ к системе либо компрометацию ключевой/парольной информации, незамедлительно сообщить об этом в Банк по официальному телефону, а затем лично в письменной форме;
4.1.6. завершать работу систем ДБО. в соответствии с установленными процедурами. Не допускается закрытия окна браузера, без предварительного выхода из систем ДБО. Если Клиент не выполнял вход в системы ДБО, но при этом получил сообщение о входе в систему ДБО, незамедлительно сообщить об этом в Банк по официальному телефону, а затем лично в письменной форме.

5. Правила безопасности – использование систем ДБО на мобильных устройствах (в том числе в мобильное приложение «КББ-ОНЛАЙН /Инфосервис)

5.1. Клиент обязан:

5.1.1. Использовать на мобильных устройствах только официальные приложения, разработанные производителем соответствующей системы ДБО.

5.1.1. Не использовать несанкционированные модификации программного обеспечения мобильных устройств (взлом прошивки, rooting, jailbreaking).

5.1.3. Не использовать мобильные устройства для доступа к полнофункциональным версиям систем ДБО.

6. Правила безопасности – банковская карта.

6.1. При использовании банковской карты в банкоматах, иных устройствах самообслуживания (далее по тексту – УСО) Клиент обязан убедиться в безопасности такого УСО.

6.2. При использовании данных банковской карты в сети Интернет Клиент обязан соблюдать требования и рекомендации, изложенные в разделах 3,4,5 Порядка.

6.3. Клиент обязан не использовать УСО если:

6.3.1. УСО не находится в безопасном месте;

6.3.2. УСО содержит дополнительные устройства, не соответствующие конструкции УСО или расположенные в месте набора ПИН-кода или в месте приема банковской карты;

6.3.3. в непосредственной близости от УСО находятся посторонние лица.

6.4. Клиент обязан:

6.4.1. установить ПИН–код, так чтобы его невозможно было угадать или подобрать;

6.4.2. не записывать/не разглашать ПИН-код;

6.4.3. регулярно менять ПИН-код через УСО банка, при этом ПИН-код не должен повторяться;

6.4.4. при использовании банковской карты пользоваться УСО Банка;

6.4.5. набирать ПИН-код на клавиатуре УСО несколькими пальцами быстрыми движениями, прикрывая клавиатуру другой рукой;

6.4.6. не записывать на банковской карте денежных средств больше, чем будет необходимо в ближайшее время для совершения операций с использованием банковской карты;

6.4.7. в случае, если ПИН–код стал или мог стать известен третьим лицам, если банковская карта не была возвращена УСО, Клиент обязан сообщить об этом в Банк по телефону, а затем лично в письменной форме;

6.4.8. при получении банковской карты подписать ее на оборотной стороне;

6.4.9. держать банковскую карту в недоступном для третьих лиц месте и не допускать ее несанкционированного использования третьими лицами;

6.4.10. использовать банковскую карту строго по назначению;

6.4.11. не допускать использования чеков и других документов, на которых указан номер банковской карты и/или счета в Банке, посторонними лицами.

6.5. Клиент соглашается с тем, что:

6.5.1. Использование банковской карты и введение правильного ПИН-кода при проведении банковских операций через УСО/терминал и/или при оплате товаров, работ и услуг с использованием банковской карты Клиента является надлежащей и достаточной идентификацией Клиента;

6.5.2. ПИН-код является подтверждением для проведения банковских операций по счетам Клиента;

6.5.3. В случае использования УСО/терминала другого банка, Банк не несет ответственности за безопасность использования такого УСО/терминала.

6.5.4. Вне зависимости от факта утраты карточки, времени получения банком информации об утрате карточки, Клиент несет ответственность за операции с карточкой, совершенные третьими лицами с ведома Клиента, а также с использованием его PIN-кода.

7. Оспаривание операций

7.1. В случае если по счету Клиента была совершена несанкционированная операция, Клиенту необходимо подать заявление в письменной форме в Банк и в правоохранительные органы о совершении несанкционированной операции по счету Клиента.

7.2. В случае если Клиентом обнаружена спорная/подозрительная ситуация, связанная со счетами Клиента в Банке, необходимо уведомить об этом Банк через службу обратной связи на сайте банка в сети Интернет. Если возникшую спорную ситуацию невозможно урегулировать с представителем Банка через службу обратной связи на сайте банка в сети Интернет, Клиенту необходимо предоставить в офис Банка письменное заявление о возникшей спорной ситуации.

7.3. Для урегулирования возникшей ситуации (в т.ч. связанной несанкционированными операциями) Банк вправе пригласить Клиента на личную встречу с уполномоченным сотрудником Банка. В случае необходимости урегулирования возникшей спорной ситуации Банк может привлекать различных специалистов и экспертов (как являющихся, так и не являющихся сотрудниками Банка).

7.4. Банк обязан рассматривать заявление Клиента, в том числе при возникновении споров, связанных с использованием Клиентом его электронного средства платежа. Банк принимает все возможные меры по урегулированию возникшей спорной ситуации. Срок рассмотрения заявления составляет 30 дней со дня получения таких заявлений относительно использования электронного средства платежа в инфраструктуре на территории РФ и 60 дней со дня получения заявлений в случае использования электронного средства платежа в инфраструктуре за пределами РФ. Клиент вправе получать информацию о ходе рассмотрения его письменного заявления через службу обратной связи на сайте банка в сети Интернет либо по желанию клиента, путем получения ответа в письменной форме по указанному в заявлении адресу. В случае принятия банком решения о возврате денежных средств, возврат осуществляется Банком не позднее 7 рабочих дней со дня принятия Банком решения о возврате.
7.5. Банк вправе запросить, а Клиент обязан по запросу Банка предоставить все имеющиеся доказательства, подтверждающие наличие обстоятельств несанкционированного использования электронного средства платежа, компрометацию ключевой/парольной информации.
7.6. Банк вправе запросить, а Клиент обязан по запросу Банка предоставить всю имеющеюся информацию относительно использования электронного средства платежа, ключевой/парольной информации, компьютеров или иных устройств.
7.7. В период рассмотрения спорной ситуации относительно использования электронного средства платежа, Банк вправе приостановить либо прекратить использование электронного средства платежа. Указанные действия Банка не прекращают действие договора банковского счета.
7.8. При осуществлении оплаты за товары и услуги с использованием банковской карты идентификация Клиента и установление его личности должны производиться соответствующим предприятием торговли и обслуживания, принимающим банковскую карту к оплате. Банк не несет ответственности за нарушение предприятием торговли и обслуживания порядка идентификации держателя банковской карты и установления его личности, и Клиент не вправе предъявлять Банку какие-либо претензии в этой связи.
7.9. Операции, совершенные посредством электронного средства платежа:
7.9.1. подтвержденные ПИН-кодом/CVV2/CVC2/ППК2;
7.9.2. с применением ключевой или парольной информации;
7.9.3. с использованием SMS-сообщений, отправленных с телефонных номеров, предоставленных Клиентом при подключении к соответствующим услугам, в том числе с использованием банковской карты;
не признаются как «несанкционированные операции» либо как «операции, совершенные без согласия Клиента» и не могут быть опротестованы. Клиент обязан использовать предлагаемые Банком технологии для более безопасного использования электронного средства платежа.
7.10. В случае, не получения сообщения банка, операции с использованием электронных средств платежа, по которым в Банк не поступило письменно оформленной претензии до истечения последнего рабочего дня месяца, следующего за месяцем отражения операции по Счету Клиента, считаются подтвержденными Клиентом.
7.11. Клиент единолично несет ответственность за соблюдение всех требований и рекомендаций, изложенных в настоящем Порядке. В случае нарушения настоящего Порядка, а также не уведомления Банка об утрате электронного средства платежа/компрометации ключевой информации/компрометации парольной информации и/или использования электронного средства платежа/ключевой информации/парольной информации без согласия Клиента, повлекшего за собой совершение несанкционированной операции по счету Клиента, Клиент не вправе предъявлять Банку какие-либо претензии по такой несанкционированной операции, и Банк не должен их рассматривать.

8. Дополнительные условия

8.1. При невозможности выполнения со стороны Клиента всех указанных требований и рекомендаций, для обеспечения сохранности своих денежных средств, Клиенту следует осуществлять банковские операции в офисах Банка.
8.2. При поступлении Клиенту сообщения о несанкционированном использовании электронного средства платежа Клиент обязан сообщить об этом в Банк по телефону при наличии кодового слова, а затем лично в письменной форме. Для связи с Банком Клиент обязан использовать только контактную информацию Банка, указанную на официальном сайте Банка в сети Интернет.