Приложение № 5
к Приказу № 1240 от 24.07.2024

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. Термины и определения

Банк – ООО КБ «РостФинанс».

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

ДБО – Система дистанционного банковского обслуживания.

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 Онлайн-банка.

Средство подтверждения – средство дополнительного подтверждения Клиентом передаваемого по системе ДБО распоряжения. Формируется системой ДБО и направляется Клиенту (Представителю клиента) на указанный им номер мобильного телефона посредством SMS-сообщения/Push-ведомления для удостоверения права распоряжения средствами на счетах при совершении операций.

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 мобильных устройств. Сервис «SMS-информирование»/ «Pushуведомления» предоставляется в рамках услуги обслуживания счетов с использованием системы ДБО, с использованием Банковской карты и (или) ее реквизитов. Данный сервис предназначен для информирования Клиентов о совершенных операциях по их счетам или банковским картам, о размере и сроках обязательных ежемесячных платежей по кредитным договорам, о новых продуктах и услугах.

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, работникам 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 работника 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 работникам 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 банкноты 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 работника 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 23 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:

- **MS 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 работника 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 Системы ДБО.

При работе в системе ДБО адрес сайта должен начинаться: https://online.rostfinance.ru/

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 операционная система, антивирусное программное обеспечение с актуальными антивирусными базами.

- 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 работник Банка 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 официальный телефон 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, работниками 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. работникам Банка) идентификаторов своих рабочих мест и принятия согласия на подключение третьих лиц (в т.ч. работников Банка) к своим рабочим места.

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

Возобновление обслуживание (начало обслуживания) клиента с использованием технологии дистанционного доступа к банковскому счету (включая интернет-банкинг) производится при условии предоставления клиентом запрошенных документов, на основании которых Банк сможет сделать вывод об отсутствии подозрений в том, что целью совершения операции является незаконный вывод денежных средств из РФ, легализация (отмывание) доходов, полученных преступным путем, или финансирование терроризма.