Приложение 2
к приказу АО «Россельхозбанк»
от 17.09.2008 № 317-ОД
(в редакции приказов АО «Россельхозбанк» от 08.07.2013 № 321-ОД, от 02.10.2014 № 600-ОД, от 17.08.2015 № 708-ОД, от 31.05.2016 № 373-ОД, от 14.07.2016 № 504-ОД, от 03.08.2016 № 558-ОД)

Памятка
держателя платежных карт АО «Россельхозбанк»

Соблюдение рекомендаций, содержащихся в Памятке, позволит обеспечить максимальную сохранность платежной карты, ее реквизитов, ПИН-кода и других данных, а также снизит возможные риски при совершении операций с использованием карты в банкомате, при оплате товаров и услуг, в том числе при использовании платежных карт через Интернет.

1. Общие рекомендации

1.1. ПИН-код должен быть известен только Вам и не может быть затребован ни Банком, ни любой другой организацией. Запрещается хранение данных о ПИН-коде на любых носителях информации.

Ввод ПИН-кода производится для подтверждения операций, проводимых в банкоматах и электронных терминалах, а также при генерации одноразовых паролей для доступа к дистанционному банковскому обслуживанию (при этом используется выдаваемое Банком специальное устройство генерации паролей) и при получении пароля для совершения операций в сети Интернет.

При проведении операции с вводом ПИН-кода прикрывайте клавиатуру свободной рукой. Это не позволит мошенникам подсмотреть Ваш ПИН-код или записать его на видеокамеру.

1.2. При самостоятельном выборе ПИН-кода не используйте простые комбинации (например, одинаковые цифры) и комбинации, связанные с вашими персональными данными (дата рождения и т.п.).

1.3. При получении электронного письма и SMS-сообщения, в которых от имени Банка предлагается предоставить персональные данные, или информацию о платежной карте (в том числе ПИН-код) не сообщайте их. Не следуйте по «ссылкам», указанным в письмах (включая ссылки на сайт Банка) и SMS-сообщениях, т.к. они могут вести на сайты-двойники и вирусоопасные сайты (сайты с повышенной опасностью заражения вирусами). Перезвоните в службу поддержки Банка и сообщите о данном факте.

1.4. В целях информационного взаимодействия с Банком рекомендуется 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.

1.5. Храните свою карту в недоступном для окружающих месте, а также отдельно от наличных денег и документов.

1.6. Не разглашайте реквизиты платежной карты (номер, срок действия и иные сведения), персональную информацию третьим лицам, за исключением случаев передачи реквизитов платежной карты при оформлении заказов по почте, телефону или через Интернет.

1.7. Не передавайте карту третьим лицам, за исключением случаев передачи карты работникам торгово-сервисных предприятий (далее – ТСП) и в пунктах выдачи наличных (далее - ПВН) при осуществлении Вами операций, в т.ч. оплаты товаров и услуг с помощью карты.

1.8. Помните, что в случае компрометации сведений о реквизитах платежной карты, ПИН-коде, 3-D-пароле, разглашения персональных данных Держателя, утраты/кражи карты

существует риск совершения неправомерных действий с денежными средствами на Вашем банковском счете (далее – Счете) со стороны третьих лиц.

1.9. Служба поддержки Банка по телефонам 8 (800)200-6099 (звонок по России бесплатный), +7(495)651-6099 КРУГЛОСУТОЧНО:

– принимает сообщения об утрате/краже карты/подозрении в неправомерном/мошенническом использовании платежной карты и консультирует о порядке действий в этих ситуациях;

– дает рекомендации о порядке действий в случае выявления спорных ситуаций или неправомерных отказов в совершении операций с использованием платежной карты, отвечает на вопросы, связанные с выпуском и обслуживанием платежных карт.

Рекомендуется всегда иметь при себе телефон Службы поддержки Банка.

1.10. Не подвергайте карту тепловому и электромагнитному воздействию, а также избегайте попадания на карту влаги. Не храните карту в портмоне или сумке с магнитной застежкой, рядом с мобильным телефоном, бытовой и офисной техникой. Не кладите карту на металлическую поверхность, не сгибайте и не царапайте ее.

Если в результате повреждения карту стало невозможно использовать при проведении операций, обратитесь в Банк для ее сдачи и получения новой карты.

2. Совершение операций с картой в банкомате

2.1. Осуществляйте операции с использованием банкоматов, установленных в безопасных местах (например, в подразделениях банков).

2.2. Дверь в помещение, где расположен банкомат, может быть оборудована электронным замком, открываемым картой. Помните, что он должен открываться без введения ПИН-кода. Если Вам предлагают ввести ПИН-код, то перед Вами устройство, установленное мошенниками.

2.3. Прежде чем провести по карте операцию через банкомат убедитесь в наличии на банкомате логотипа платежной системы, соответствующей Вашей карте, а также информации о банке, обслуживающем банкомат (название, адрес, телефон).

2.5. Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций с картой в банкоматах.

2.6. Не допускайте ошибок при вводе ПИН-кода. В случае если ПИН-код три раза подряд будет набран неверно, карта заблокируется на совершение операций с вводом ПИН-кода. В этом случае Вам необходимо обратиться в подразделение Банка для изменения ПИН-кода.

2.7. По завершении операции не забудьте забрать выданные деньги, карту и квитанцию банкомата (они могут возвращаться в любой последовательности). В случае если после проведения операции карта не была удалена из картоприемника по истечении 20-40 секунд, она будет задержана банкоматом.

2.8. Если банкомат задержал Вашу карту, Вам необходимо:

– переписать указанные на банкомате реквизиты (название, адрес и телефон) банка, которому принадлежит банкомат;

– обратиться в Службу поддержки Банка по многоканальному телефону, указанному в пункте 1.9 и действовать в соответствии с инструкциями оператора Службы поддержки.

2.9. При приеме и возврате карты банкоматом не толкайте и не выдергивайте карту до окончания ее движения в картоприемнике.

2.10. 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 карты.

2.11. После получения наличных денежных средств в банкомате следует пересчитать банкноты полистно, убедиться в том, что карта была возвращена банкоматом, дождаться выдачи

квитанции при ее запросе, затем положить их в сумку (кошелек, карман) и только после этого отходить от банкомата.

3. Рекомендации при использовании карты для оплаты товаров и услуг в торгово-сервисных предприятиях

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

3.2. Во избежание мошенничества с Вашей картой требуйте проведения операций с ней только в Вашем присутствии, не позволяйте уносить ее из поля Вашего зрения.

3.3. Кассир ТСП может потребовать предъявления документа, удостоверяющего Вашу личность. В случае отсутствия документа, Вам может быть отказано в проведении операции по карте.

3.4. При осуществлении операции в ТСП с использованием электронного терминала, кассир может предложить Вам ввести ПИН-код на выносной клавиатуре электронного терминала или на клавиатуре самого терминала. При отказе ввести ПИН-код или неверном вводе ПИН-кода в проведении операции может быть отказано.

По завершении операции кассир должен выдать Вам документ, подтверждающий проведение операции с использованием карты (далее – квитанция). Несогласие подписать квитанцию также может привести к отказу в проведении операции.

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.

3.5. Не подписывайте квитанцию, в которой не проставлены (не соответствуют действительности): вид операции, сумма операции, валюта операции, дата совершения операции, сумма комиссии (если имеет место), код авторизации, реквизиты карты, наименование ТСП.

3.6. В случае Вашего отказа от покупки сразу же после завершения операции требуйте отмены операции и убедитесь в том, что кассир ТСП уничтожил ранее оформленную квитанцию.

3.7. При возврате покупки или отказе от услуг, ранее полученных в ТСП по Вашей карте, должна быть проведена кредитовая операция – операция «возврат покупки» с обязательным оформлением квитанции, на которой должно быть указано «возврат покупки», подписанной кассиром ТСП. Непременно сохраните квитанцию на «возврат покупки». Если сумма операции не поступит на Ваш Счет в течение 15 календарных дней, обратитесь в подразделение Банка для оформления претензии.

3.9. В случае если при попытке оплаты картой имела место «неуспешная» операция, следует сохранить один экземпляр выданного терминалом чека для последующей проверки на отсутствие указанной операции в выписке по Счету.

3.10. В случае любого неправомерного, с Вашей точки зрения, отказа в проведении операции по карте рекомендуем Вам незамедлительно связаться со Службой поддержки Банка по многоканальному телефону, указанному в пункте 1.9.

4. Изъятие карты

4.1. Ваша карта может быть изъята в банкомате, ПВН, а также в ТСП в случае:

- использования карты, ранее заявленной как утраченная;
- использования карты с истекшим сроком действия;
- использования карты третьими лицами;
- использования карты после получения Вами уведомления Банка с требованием о возврате карты;
- иных случаях неправомерного использования карты, включая покупку товаров и услуг, запрещенных действующим законодательством Российской Федерации.

4.2. В случае изъятия карты в ТСП или ПВН Банка требуйте расписку об изъятии с указанием даты, времени и причины изъятия, убедитесь, что изъятая у Вас карта разрезана в Вашем присутствии. Сообщите об изъятии карты в Службу поддержки Банка по многоканальному телефону, указанному в пункте 1.9.

5. Совершение операций с платежной картой через сеть Интернет

5.1. Для обеспечения дополнительной безопасности платежных операций в сети Интернет по Картам международных платежных систем VISA International, MasterCard WorldWide в некоторых случаях требуется подтверждение операции специальным 3-D паролем. По выбору Держателя/Держателя дополнительной карты Банк предоставляет следующие способы получения 3-D пароля:

- в SMS-сообщении, направленном на номер мобильного телефона, зарегистрированный в Банке (только после подключения данного способа в соответствии с пунктом 5.2 настоящей Памятки и получения ответа на запрос, направленный в соответствии с пунктом 5.2.1 настоящей Памятки);
- в банкомате/информационно-платежном терминале Банка/системе дистанционного банковского обслуживания.

Держатель/Держатель дополнительной карты может применять любой способ получения 3-D пароля.

5.2. Банк предоставляет возможность Держателю/Держателю дополнительной карты подключить способ получения 3-D пароля посредством SMS-сообщения. Для этих целей осуществляется регистрация соответствующего номера телефона в банкомате/ информационно-платежном терминале Банка. Изменение номера мобильного телефона для получения 3-D пароля на новый номер также регистрируется Держателем/Держателем дополнительной карты в банкомате/ информационно-платежном терминале Банка.

При регистрации номера телефона для получения 3-D паролей, отличного от номера телефона, используемого для SMS-аутентификации в рамках предоставления дистанционного банковского обслуживания, а также при изменении номера мобильного телефона для получения 3-D пароля временные и одноразовые пароли для SMS-аутентификации будут направляться на номер телефона, зарегистрированный для получения 3-D пароля.

При регистрации номера телефона для получения временных и одноразовых паролей для SMS-аутентификации в рамках предоставления дистанционного банковского обслуживания, отличного от номера телефона, используемого для получения 3-D паролей, а также при изменении номера мобильного телефона для получения временных и одноразовых паролей для SMS-аутентификации 3-D пароли будут направляться на номер телефона, зарегистрированный для осуществлении SMS-аутентификации.

5.2.1. В случае необходимости получения 3-D пароля на номер мобильного телефона, Держатель/Держатель дополнительной карты направляет в Банк с зарегистрированного согласно пункту 5.2 номера мобильного телефона SMS-сообщение на номер телефона: **+7-903-767-20-90** со следующим текстом:

«3DPASSxxxx»,

где xxxx – последние 4 цифры номера его карты.

Срок действия 3-D пароля – 15 минут с момента его формирования.

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

5.4. 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.

5.5. Рекомендуется совершать покупки только со своего компьютера в целях сохранения конфиденциальности персональных данных и(или) информации о платежной карте/Счете.

5.6. Не передавайте полные реквизиты платежной карты (а также полный номер карты) через открытые электронные каналы информационного обмена – такие, как электронная почта, смс-сообщения, ICQ и т.п.

Ввод полных реквизитов платежной карты допустим только в специальную платежную форму на сайте интернет-магазина при совершении покупки.

5.7. Не осуществляйте вход в системы дистанционного банковского обслуживания в местах, где услуги Интернета являются общедоступными, с использованием публичных беспроводных сетей, например, Интернет-кафе или общественный транспорт.

5.8. В случае присоединения Держателя к Условиям дистанционного банковского обслуживания физических лиц в АО «Россельхозбанк» с использованием системы «Интернет-банк» и «Мобильный банк» для входа в системы «Интернет-банк» и «Мобильный банк» ввод номера платежной карты и ПИН-кода к ней не требуется.

В случае присоединения Держателя к Условиям дистанционного банковского обслуживания физических лиц в АО «Россельхозбанк»[1] для входа в систему «Интернет-офис» ввод полного номера платежной карты не требуется – достаточно ввести лишь последние четыре цифры номера..

5.9. Установите на свой компьютер персональные межсетевые экраны, антивирусное программное обеспечение и регулярно производите его обновление и обновление других используемых Вами программных продуктов (операционной системы и прикладных программ). Используйте программное обеспечение анализа безопасности Вашего компьютера и сайтов, которые Вы собираетесь посетить (свободно распространяемые программы от McAfee - Security Scan Plus, Site Advisor и др. программные продукты). Это может защитить Вас от проникновения вредоносного программного обеспечения.

[1] С 14.07.2016 Банк не осуществляет подключение Держателей к системам «Интернет-офис» и «Мобильный банк» в рамках Условий дистанционного банковского обслуживания физических лиц в АО «Россельхозбанк».