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, от 01.06.2017 № 308-ОД, от 29.01.2018 № 41-ОД, от 23.11.2018 № 1221-ОД, от 28.01.2019 № 74-ОД, от 20.05.2019 № 660-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 информационно-телекоммуникационную сеть 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 информационно-телекоммуникационную сеть 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.

1.11. При оформлении дополнительной карты на имя несовершеннолетнего лица рекомендуется установить индивидуальные лимиты расходования денежных средств с использованием дополнительной карты/реквизитов дополнительной карты и подключить услугу «SMS-сервис» в целях осуществления контроля расходования средств на Счете.

1.12. Банк вправе использовать все указываемые Держателем/Держателем дополнительной карты номера его телефонов для осуществления SMS-информирования и направления иной персонифицированной и неперсонифицированной информации, в случаях, определенных Условиями комплексного банковского обслуживания держателей карт АО «Россельхозбанк» (далее – Условия), а также для осуществления телефонного звонка в целях подтверждения авторства операции в соответствии с пунктом 7.3.9 Условий, и для информирования о получения сведений о компрометации реквизитов платежной карты и/или ПИН-кода**.**

1.13. Банк приостанавливает/отказывает в проведении операции по карте/дополнительной карте[1] для проведения контроля в целях предотвращения осуществления перевода денежных средств без согласия клиента **в случае,** если:

2. Банк при проведении контроля распоряжения выявил признаки перевода денежных средств без согласия клиента;

3. у Банка имеются основания предполагать, что электронными средствами платежа распоряжается неуполномоченное лицо;

4. Банком выявлены факты, что реквизиты платежной карты, ПИН-код, 3-D пароль скомпрометированы и/или выявлен неподтверждённый клиентом факт смены SIM-карты номера мобильного телефона для 3-D пароля, а также в случае принадлежности номера мобильного телефона для 3-D пароля третьему лицу, завладения третьим лицом мобильным телефоном Держателя/Держателя дополнительной карты или иного отчуждения номера для получения 3-D паролей и/или мобильного телефона.

[1] В соответствии с требованиями Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе».

В случае приостановки перевода или отказа в совершении операции Банк уведомляет Держателя/Держателя дополнительной карты о данном событии в виде SMS-информирования и/или E-mail-уведомления и/или путем телефонного звонка работника Банка Держателю/Держателю дополнительной карты[2] и запрашивает у него подтверждение факта осуществления операции или формирования распоряжения лично Держателем/ Держателем дополнительной карты, а также предоставляет Держателю/Держателю дополнительной карты рекомендации по снижению рисков повторного осуществления перевода денежных средств без его согласия.

Подтвердить авторство распоряжения Держатель/Держатель дополнительной карты может, обратившись в Службу поддержки Банка.

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.

---

[2] Способ уведомления и выбор номера для отправки SMS-информирования и/или осуществления звонка определяется Банком самостоятельно.

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 информационно-телекоммуникационную сеть Интернет

5.1. Для обеспечения дополнительной безопасности платежных операций в информационно-телекоммуникационной сети Интернет по Картам международных платежных систем VISA International, MasterCard WorldWide, UnionPay International и платежной системы МИР требуется подтверждение операции специальным 3-D паролем.

Банк либо международная платежная система UnionPay International направляет 3-D пароли Держателю/Держателю дополнительной карты в SMS-сообщении, направленном на номер мобильного телефона, зарегистрированном в Банке для получения 3-D паролей в соответствии с пунктом 5.2 настоящей Памятки.

Банк предоставляет Держателю/Держателю дополнительной карты 3-D пароли посредством SMS-сообщений по Картам международных платежных систем VISA International, MasterCard WorldWide и платежной системы МИР, выпущенным на имя Держателя/Держателя дополнительной карты.

Международная платежная система UnionPay International предоставляет Держателю/Держателю дополнительной карты 3-D пароли посредством SMS-сообщений по Картам международной платежной системы UnionPay International, выпущенным на имя Держателя/Держателя дополнительной карты.

5.2. Банк предоставляет возможность Держателю/Держателю дополнительной карты зарегистрировать соответствующий номер мобильного телефона для получения 3-D пароля посредством SMS-сообщения, SMS-уведомлений, использования дополнительной услуги «SMS-сервис» и передачи иной персонифицированной и неперсонифицированной информации, в случаях, определенных Условиями комплексного банковского обслуживания держателей карт АО «Россельхозбанк». Банк предоставляет возможность Держателю/Держателю дополнительной карты указать свой номер мобильного телефона в банкомате/информационно-платежном терминале Банка или при личном обращении Держателя/Держателя дополнительной карты в подразделение Банка и заполнения соответствующего заявления по форме 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 или посредством личного обращения Держателя/Держателя дополнительной карты в подразделение Банка и заполнения соответствующего заявления по форме Банка.

При регистрации номера телефона для получения 3-D паролей на данный номер будут направляться SMS-сообщения, содержащие информацию о 3-D паролях, которые могут быть указаны Держателем/ Держателем дополнительной карты при совершении им операций по Картам международных платежных систем VISA International, MasterCard WorldWide, UnionPay International и платежной системы МИР, выпущенным на имя Держателя/Держателя дополнительной карты.

В случае изменения номера мобильного телефона для получения 3-D пароля незамедлительно предоставляйте в Банк актуальные сведения в форме письменного заявления, переданного в подразделение Банка, обслуживающее Счет, либо посредством дистанционных каналов обслуживания. Информируйте Банк о прекращении использования SIM-карты номера мобильного телефона для получения 3-D паролей – незамедлительно направляйте в Банк соответствующее уведомление, обратившись в Службу поддержки Банка, подразделение Банка, обслуживающее Счет, или сообщайте в устной форме работнику Банка, позвонившему для подтверждения авторства операции по карте. При непоступлении информации в соответствии с п.

7.2.9 Условий в течение 10 календарных дней с момента передачи Держателем/Держателем дополнительной карты в Банк распоряжения, сформированного с использованием электронных средств платежа, изменение SIM-карты номера для получения 3-D паролей считается произведенным лично Держателем/Держателем дополнительной карты.

5.3. Срок действия 3-D пароля, полученного посредством SMS-сообщения, составляет 15 минут с момента его формирования и его действие распространяется только для одной операции, в процессе совершения которой данный 3-D пароль был получен.

5.4. При совершении операции на странице ТСП с использованием реквизитов платежной карты UnionPay в информационно-телекоммуникационной сети Интернет Держатель/Держатель дополнительной карты должен указать запрашиваемые ТСП реквизиты платежной карты UnionPay.

После ввода на странице ТСП в информационно-телекоммуникационной сети Интернет реквизитов платежной карты UnionPay Держатель/Держатель дополнительной карты автоматически переходит на страницу авторизации международной платежной системы UnionPay International, на которой Держателю/Держателю дополнительной карты необходимо ввести номер мобильного телефона, зарегистрированного в Банке для получения 3-D паролей в соответствии с пунктом 5.2 настоящей Памятки.

Для подтверждения операции с использованием реквизитов платежной карты UnionPay международная платежная система UnionPay International направляет на номер мобильного телефона Держателя/Держателя дополнительной карты одноразовый 3-D пароль.

Держатель/Держатель дополнительной карты подтверждает операцию полученным от международной платежной системы UnionPay International 3-D паролем. Операция с использованием реквизитов платежной карты UnionPay в ТСП может быть проведена только в случае ввода Держателем/Держателем дополнительной карты корректного 3-D пароля.

Количество попыток, которые предоставляет международная платежная система UnionPay International Держателю/Держателю дополнительной карты на ввод 3-D пароля - 3 (Три). После 3 (Третьей) неуспешной попытки ввода Держателем/Держателем дополнительной карты 3-D пароля операция считается неподтвержденной, и Держатель/Держатель дополнительной карты возвращается на страницу ТСП в информационно-телекоммуникационной сети Интернет. Если Держатель/Держатель дополнительной карты направляет запрос на получение 3-D пароля 3 (Три) раза в течение 1 (Одного) часа, отправка нового 3-D пароля блокируется международной платежной системой UnionPay International на 1 (Один) час.

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

5.6. 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.

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

5.8. 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.

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

5.10. 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.

5.11. 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.