ПАМЯТКА
«О МЕРАХ БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ БАНКОВСКИХ КАРТ»

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

1. Общие рекомендации

1.1. Никогда не сообщайте ПИН-код третьим лицам, в том числе родственникам, знакомым, сотрудникам кредитной организации, и лицам, помогающим Вам в использовании банковской карты.

1.2. ПИН-код необходимо запомнить или в исключительных случаях, хранить его отдельно от банковской карты в неявном виде и недоступном для третьих лиц (в том числе родственников) месте.

1.3. Никогда ни при каких обстоятельствах не передавайте банковскую карту или ее реквизиты для использования третьим лицам (в том числе родственникам). Если на банковской карте нанесены фамилия и имя физического лица, то только это физическое лицо имеет право использовать банковскую карту.

1.4. При получении банковской карты распишитесь на ее оборотной стороне в месте, предназначенном для подписи держателя банковской карты, если это предусмотрено. Это снизит риск использования банковской карты без Вашего согласия в случае ее утраты.

1.5. Будьте внимательны к условиям хранения и использования банковской карты. Не подвергайте банковскую карту механическим, температурным и электромагнитным воздействиям, а также избегайте попадания на нее влаги. Банковскую карту нельзя хранить рядом с мобильным телефоном, бытовой и офисной техникой.

1.6. Телефон АО АИКБ «Енисейский объединенный банк» (далее – Банк) указан на оборотной стороне банковской карты. Кроме того, рекомендуется иметь при себе контактные телефоны Банка и номер банковской карты на других носителях информации: в записной книжке, мобильном телефоне и/или других носителях информации, но не рядом с записью о ПИН-коде.

1.7. С целью предотвращения мошеннических действий по снятию всей суммы денежных средств с банковского счета Вы можете установить суточный лимит в сумме, меньшей, чем установлено Тарифами Банка, для совершения операций по банковской карте и подключить услуги по SMS информированию (SMS-Банк) и/или дистанционному банковскому обслуживанию в системе Faktura (TEL-Банк).

1.8. Если Вы обнаружили, что не работает мобильный телефон, используемый для получения сообщений от Банка (например, без видимых причин на длительное время пропала связь), незамедлительно обратитесь в Банк и заблокируйте банковскую карту.

1.9. Принимайте меры для предотвращения риска изготовления дубликата Вашей сим-карты:

- пользуйтесь номером телефона, который оформлен лично на Вас,
- не используйте анонимные сим-карты,
- не передавайте мобильный телефон или сим-карту в пользование третьим лицам,
- обратитесь к Вашему мобильному оператору для запрета выпуска дубликатов сим-карты, а также совершения действий с Вашей сим-картой на основании доверенности.

1.10. В случае подозрения на компрометацию банковской карты, например, если карта находилась или могла находиться в руках третьего лица, незамедлительно обратитесь в Банк и заблокируйте банковскую карту.

1.11. При получении просьбы по телефону, в том числе со стороны сотрудника Банка, или посредством SMS сообщений, предоставить ПИН-код, код безопасности (CVC-код) не сообщайте их. В случае получении просьбы предоставить персональные данные или информацию о банковской карте (номер, срок действия, имя держателя карты) спросите фамилию, имя, отчество сотрудника и перезвоните в Банк по телефону, указанному на оборотной стороне банковской карты, и попросите соединить с ранее звонившим сотрудником Банка.

1.12. Не рекомендуется отвечать на электронные письма, в которых от имени Банка предлагается предоставить персональные данные. Не следуйте по «ссылкам», указанным в письмах (включая

ссылки на сайт «Банка»), т.к. они могут вести на сайты-двойники. Официальные сайты кредитных организаций в поисковых системах Яндекс и Mail.ru обозначаются знаком:

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

1.14. Помните, что в случае раскрытия ПИН-кода, персональных данных, утраты банковской карты существует риск совершения неправомерных действий с денежными средствами на Вашем банковском счете со стороны третьих лиц.

1.15. В случае если имеются предположения о раскрытии ПИН-кода, реквизитов банковской карты, персональных данных, позволяющих совершить неправомерные действия с Вашим банковским счетом, а также если банковская карта была утрачена, необходимо немедленно обратиться в Банк для осуществления блокировки Вашей банковской карты, и следовать дальнейшим указаниям сотрудника. До момента обращения в Банк Вы несете риск, связанный с несанкционированным списанием денежных средств с Вашего банковского счета. Денежные средства, списанные с Вашего банковского счета в результате несанкционированного использования Вашей банковской карты или ее реквизитов до момента уведомления об этом Банка, не возмещаются.
ВНИМАНИЕ! Для своевременной блокировки Вашей банковской карты следует обращаться в Банк по телефонам **8 (391) 277-00-00, 8 (800) 200-97-00**, либо в Процессинговый центр «КартСтандарт» по номеру **8 (800) 200-45-75.**

2. Рекомендации при совершении операций с банковской картой в банкомате

2.1. Осуществляйте операции с использованием банкоматов, установленных в безопасных местах (например, в государственных учреждениях, подразделениях банков, крупных торговых комплексах, гостиницах, аэропортах и т.п.). Информация о расположении банкоматов размещается на официальном сайте кредитной организации.

2.2. Не используйте устройства, которые требуют ввода ПИН-кода для доступа в помещение, где расположен банкомат.

2.3. В случае если поблизости от банкомата находятся подозрительные посторонние лица, следует выбрать более подходящее время для использования банкомата или воспользоваться другим банкоматом.

2.4. 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 карт (например, наличие неровно установленной клавиатуры для набора ПИН-кода).

2.5. В случае если клавиатура или место для приема карт банкомата оборудованы дополнительными устройствами, не соответствующими его конструкции, воздержитесь от использования банковской карты в данном банкомате и сообщите о своих подозрениях сотрудникам кредитной организации по телефону, указанному на банкомате.

2.6. Не применяйте физическую силу, чтобы вставить банковскую карту в банкомат. Если банковская карта не вставляется, воздержитесь от использования такого банкомата.

2.7. Наклейки на банкомате содержат торговые марки платежных систем и категорий банковских карт, которые принимаются к обслуживанию в данном устройстве. Используйте банкомат, на котором размещена информация, соответствующая Вашей банковской карте.

2.8. Рекомендуем последовательно выполнять команды, появляющиеся на экране банкомата в процессе совершения операции.

2.9. Набирайте ПИН-код таким образом, чтобы люди, находящиеся в непосредственной близости, не смогли его увидеть. При наборе ПИН-кода прикрывайте клавиатуру рукой.
ВНИМАНИЕ! Если Вы ввели неверный ПИН-код 3 раза подряд, банкомат блокирует банковскую карту. Если Вы не уверены в правильности ПИН-кода, рекомендуем отказаться от совершения операции до уточнения ПИН-кода. В случае блокировки банковской карты, информация о возможности ее разблокировки доступна по телефонам Банка 8 (391) 277-00-00 или 8 (800) 200-97-00.

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 банковской карты.

2.11. По завершении операции следует незамедлительно забрать из банкомата банковскую карту и денежные средства (при получении наличных средств).
ВНИМАНИЕ! Время для получения банковской карты и денежных средств из банкомата ограничено. Возврат денежных средств и карты сопровождается звуковым предупреждением и подачей светового сигнала (за исключением отдельных видов банкоматов). Если по какой-либо причине Вы не забрали банковскую карту или выданные деньги, они автоматически удерживаются банкоматом в целях обеспечения их сохранности. По вопросам возврата удержанной банковской карты или денежных средств Вы можете обратиться по телефонам Банка 8 (391) 277-00-00 или 8 (800) 200-97-00.

2.12. После получения наличных денежных средств в банкомате следует пересчитать банкноты, 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.

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

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

2.15. Если при проведении операций с банковской картой банкомат не возвращает банковскую карту, следует позвонить в кредитную организацию по телефону, указанному на банкомате, и объяснить обстоятельства произошедшего, а также следует обратиться в Банк, и далее следовать инструкциям сотрудника Банка

.

3. Рекомендации при использовании банковской карты для безналичной оплаты товаров и услуг

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

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

3.3. 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.

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

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

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

4.2. Не сообщайте персональные данные или информацию о банковской(ом) карте (счете) через сеть Интернет, например ПИН-код, пароли доступа к системе дистанционного банковского обслуживания Faktura, срок действия банковской карты, платежный лимит, историю операций, персональные данные.

4.3. 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.

4.4. При совершении операций через интернет-сайты, которые сертифицированы международной платежной системой Mastercard на технологию «3D Secure», необходимо ввести одноразовый пароль (предоставляется в виде SMS-сообщения / Push-уведомления на мобильный телефон).
Вы узнаете сертифицированные интернет-сайты по наличию следующих логотипов:

4.5. Никогда и никому не сообщайте полученный одноразовый пароль («3D Secure», MIRAccept) для подтверждения операции.

4.6. Обращайте внимание на правильность адреса страницы Банка, с которой осуществляете ввод одноразового пароля (https://acs.cardstandard.ru), т.к. похожие адреса могут использоваться третьими лицами для осуществления неправомерных действий с Вашими банковскими счетами/картами.

4.7. Обязательно сообщайте в Банк об изменении Вашего номера мобильного телефона, который был указан при подключении услуги «3D Secure» для совершения интернет-платежей с использованием банковской карты, а также в случае утери мобильного устройства и/или SIM-карты.

4.8. Рекомендуется пользоваться официальными интернет-сайтами организаций для оплаты товаров и услуг.

4.9. 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.

4.10. Рекомендуется совершать покупки только со своего компьютера / мобильного устройства в целях сохранения конфиденциальности персональных данных и (или) информации о банковской(ом) карте (счете).

4.11. 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 web-страницу продавца, на которой совершались покупки).

4.12. Установите на свой компьютер / мобильное устройство антивирусное программное обеспечение и регулярно производите его обновление и обновление других используемых Вами программных продуктов (операционной системы и прикладных программ), это может защитить Вас от проникновения вредоносного программного обеспечения.