

## Памятка по безопасному использованию банковских карт.

### Мошенничество с банковскими картами

Чтобы использовать вашу карту в своих целях, мошенникам нужно узнать ее номер, имя владельца, срок действия, номер CVC или CVV. Они могут установить скиммер на банкомат (специальное устройство, которое накладывают на приемник карты в банкомате) и видеокамеру над клавиатурой.



Для того чтобы не стать жертвой финансовых мошенников и свести к минимуму различные махинации с использованием банковской карты потребителю не следует распространять секретную информацию о карте, а также соблюдать советы по безопасному использованию банковских карт.

Соблюдение указанных ниже рекомендаций, позволит обеспечить максимальную сохранность банковской карты и ее данных, а также снизит возможные риски при совершении операций с использованием банковской карты.

Полный текст рекомендации по безопасному использованию пластиковых карт содержится в Приложении к письму ЦБР от 2 октября 2009 г. N 120-Т «О мерах безопасного использования банковских карт».

### Общие рекомендации.

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

✓ ПИН необходимо запомнить 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.

✓ Никогда ни при каких обстоятельствах не передавайте банковскую карту 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.

✓ 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.

✓ С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковского счета целесообразно 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).

✓ При получении просьбы, в том числе со стороны сотрудника кредитной организации, сообщить персональные данные или информацию о банковской карте не сообщайте их. Позвоните в кредитную организацию, выдавшую банковскую карту и сообщите о данном факте.

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



✓ В случае если имеются предположения о раскрытии ПИН, персональных данных, позволяющих совершить неправомерные действия с Вашим банковским счетом, а также если банковская карта была утрачена, необходимо немедленно обратиться в кредитную организацию, выдавшую банковскую карту, и следовать указаниям сотрудника данной кредитной организации. До момента обращения в банк Вы несете риск, связанный с несанкционированным списанием денежных средств с Вашего банковского счета. Как правило, согласно условиям договора с кредитной организацией, выдавшей банковскую карту денежные средства, списанные с Вашего банковского счета в результате несанкционированного использования Вашей банковской карты до момента уведомления об этом кредитной организации, не возмещаются.



### **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, которые требуют ввода ПИН для доступа в помещение, где расположен банкомат.

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

❖ Перед использованием банкомата осмотрите его на наличие дополнительных устройств, не соответствующих его конструкции и расположенных в месте набора ПИН и в месте (прорезь), предназначенном для приема карт (например, наличие неровно установленной клавиатуры набора ПИН). В указанном случае воздержитесь от использования такого банкомата.

❖ 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.

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

❖ Набирайте ПИН таким образом, чтобы люди, находящиеся в непосредственной близости, не смогли его увидеть. При наборе ПИН прикрывайте клавиатуру рукой.

❖ После получения наличных денежных средств в банкомате следует пересчитать банкноты поштучно, убедиться в том, что банковская карта была возвращена банкоматом, дождаться выдачи квитанции при ее запросе, затем положить их в кошелек и только после этого отходить от банкомата.

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

❖ Если при проведении операций с банковской картой в банкомате банкомат не возвращает банковскую карту, следует позвонить в кредитную организацию по телефону, указанному на банкомате, и объяснить обстоятельства произошедшего, а также следует обратиться в кредитную организацию, выдавшую банковскую карту, которая не была возвращена банкоматом, и далее следовать инструкциям сотрудника кредитной организации.

### **Рекомендации при использовании банковской карты для безналичной оплаты 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, 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. Перед набором ПИН 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.

✓ 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.

### **Рекомендации при совершении операций с банковской картой через сеть Интернет**

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

❖ Не сообщайте персональные данные или информацию о банковской(ом) карте (счете) через сеть Интернет, например ПИН, 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.

❖ Рекомендуется совершать покупки только со своего компьютера в целях сохранения конфиденциальности персональных данных и(или) информации о банковской(ом) карте (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 web-страницу продавца, на которой совершались покупки).

❖ Установите на свой компьютер 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.

