ПАМЯТКА
О МЕРАХ БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ БАНКОВСКИХ КАРТ «VISA»/«Мир»

Уважаемый клиент!

Вы стали владельцем банковской карты (далее – «банковская карта»). Пожалуйста, внимательно прочтите эту краткую Памятку.

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 (устройствах самообслуживания), при безналичной оплате товаров и услуг, в том числе через сеть Интернет.

Общие рекомендации

1. Никогда не сообщайте ПИН-код третьим лицам, в том числе родственникам, знакомым, сотрудникам кредитной организации, кассирам и лицам, помогающим Вам в использовании банковской карты.
2. ПИН-код 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.
3. 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.
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.
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.
6. Телефон кредитной организации - эмитента банковской карты (кредитной организации, выдавшей банковскую карту) указан на оборотной стороне банковской карты. Также необходимо всегда иметь при себе контактные телефоны кредитной организации - эмитента банковской карты 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.
7. С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с карточного 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).
8. При получении просьбы, в том числе со стороны сотрудника кредитной организации, сообщить персональные данные или информацию о банковской карте (в том числе ПИН-код) не сообщайте их. Перезвоните в кредитную организацию - эмитент банковской карты (кредитную организацию, выдавшую банковскую карту) и сообщите о данном факте.
9. Не рекомендуется отвечать на электронные письма, в которых от имени кредитной организации (в том числе кредитной организации - эмитента банковской карты (кредитной организации, выдавшей банковскую карту)) предлагается предоставить персональные данные. Не следуйте по «ссылкам», указанным в письмах (включая ссылки на сайт кредитной организации), т.к. они могут вести на сайты-двойники.
10. В целях информационного взаимодействия с кредитной организацией - эмитентом банковской карты (кредит-ной организации, выдавшей банковскую карту) 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 кредитной организации - эмитенте банковской карты.

Телефоны круглосуточной службы поддержки держателей карты «VISA»/«Мир» указаны на оборотной стороне банковской карты. Телефоны клиентских подразделений АКБ «Ланта-Банк» (АО)/его филиалов указаны на сайте банка (при выдаче банковской карты в филиале АКБ «Ланта-Банк» (АО) используется соответствующий раздел сайта).

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

В случае если имеются предположения о раскрытии ПИН-кода, персональных данных, позволяющих совершить неправомерные действия с Вашим карточным счетом, а также, если банковская карта была утрачена, **необходимо обратиться в круглосуточную службу поддержки: для держателей карт «VISA» по телефону (495) 785-15-15 или 8-800-200-30-22; для держателей карт «Мир» по телефону 8 800 100 54 64 или * 5464 с мобильного**, либо в рабочие часы в клиентское подразделение АКБ «Ланта-Банк» (АО)/его филиалов для немедленной блокировки банковской карты. До момента блокировки банковской карты Вы несете риск, связанный с несанкционированным списанием денежных средств с Вашего карточного счета.

Информация о действиях клиента в случае утраты банковской карты либо несанкционированного доступа к ней указана в документе АКБ «Ланта-Банк» (АО) «Условия и порядок осуществления перевода денежных средств/драгоценных металлов по поручениям физических и юридических лиц, индивидуальных предпринимателей по их банковским, карточным счетам, счетам по вкладам (депозитам) в АКБ «Ланта-Банк» (АО)». Указанный документ размещен на сайте АКБ «Ланта-Банк» (АО) (в разделе соответствующего филиала), а также во всех клиентских залах обслуживания АКБ «Ланта-Банк» (АО).

12. Для получения от Банка уведомлений о совершенных операциях используйте sim-карты и email-адреса, которые оформлены только лично на вас.
13. Не приобретайте sim-карты у неизвестного продавца, неуполномоченного оператором мобильной связи к продаже sim--карт.
14. По возможности имейте отдельные sim-карту или email-адрес для получения сообщений/уведомлений по операциям, совершаемым с использованием карты.

15. Позаботьтесь о том, чтобы на вашем телефоне не было установлено никаких лишних приложений. Обязательно установите на свой телефон антивирус. Все приложения необходимо устанавливать только по ссылкам из проверенных источников.
16. Не давайте свой телефон, sim-карту, email-адрес для пользования другим лицам.
17. Старайтесь не указывать номер своего телефона или email-адрес, используемые для работы с картой, в социальных сетях.
18. Воспользуйтесь услугой вашего оператора сотовой связи на запрет совершения действий с вашей sim-картой по доверенности (такую услугу предлагают, в частности, Мегафон, Теле2, Билайн).
19. Не отвечайте на sms- или email –сообщения, в которых якобы от имени кредитной организации сообщается о каких-либо действиях с банковской картой и предлагается перезвонить по указанному в сообщении мобильному телефону с целью «решения проблемы». Это мошеннические рассылки с целью инициировать звонок от клиента и затем узнать у него в разговоре данные о пластиковой карте или даже убедить его произвести какие-либо действия (подойти к банкомату, опять позвонить мошенникам и по инструкции по телефону нажать какие-то клавиши). Запомните, что все сообщения от банка (АКБ «Ланта-Банк» (АО)) в рамках услуги sms-информирования приходят только с номера с идентификатором Lanta-Bank.
20. Знайте, что Банк не запрашивает через sms или email какие-либо пароли для отмены операций, а также не направляет sms или email-сообщения с просьбой подтвердить, обновить или предоставить следующие данные: номер телефона, номера банковских карт и иные реквизиты карты, данные документа удостоверяющего личность, ПИН-коды, CVV, кодовое слово и т.д. Указанные действия могут исходить от мошенников.
21. В случае утраты sim-карты, либо когда невозможно достоверно установить, что произошло с sim-картой, незамедлительно обращайтесь к оператору сотовой связи для блокировки sim-карты, а также в Банк для блокировки дистанционных услуг (в том числе, карты), для оказания которых используется номер мобильного телефона.
22. Помните, что Банк не направляет email-сообщения, в которых под различными предлогами просит Вас открыть файл-вложение, или перейти по непонятной ссылке для загрузки файла. Как правило, такие файлы и ссылки содержат вирус.
23. Помните, что Банк также не направляет email-сообщения, в которых: есть ссылка на сайт банка, при этом URL-адрес ссылки отличается от официального адреса (www.lanta.ru) Банка. При входе на сайт, замаскированный под официальный сайт Банка, могут появляться всплывающие окна, в которых запрашивается ввод или подтверждение Ваших персональных данных; к сообщению прилагается файл-вложение, который Вам настойчиво рекомендуют открыть; в тексте сообщения содержатся явные и (или) многократные опечатки или орфографические ошибки.

Рекомендации при совершении операций с банковской картой в банкомате (устройстве самообслуживания)

1. Осуществляйте операции с использованием банкоматов (устройств самообслуживания), установленных в безопасных местах (например, в государственных учреждениях, подразделениях банков, крупных торговых комплексах, гостиницах, аэропортах и т.п.).
2. Не используйте устройства, которые требуют ввода ПИН-кода для доступа в помещение, где расположен банкомат.
3. В случае если поблизости от банкомата находятся посторонние лица, следует выбрать более подходящее время для использования банкомата или воспользоваться другим банкоматом.
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 набора ПИН-кода). В указанном случае воздержитесь от использования такого банкомата.
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.
6. Не применяйте физическую силу, чтобы вставить банковскую карту в банкомат. Если банковская карта не вставляется, воздержитесь от использования такого банкомата.
7. Набирайте ПИН-код таким образом, чтобы люди, находящиеся в непосредственной близости, не смогли его увидеть. При наборе ПИН-кода прикрывайте клавиатуру рукой.
8. 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.
9. 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 их в сумку (кошелек, карман) и только после этого отходить от банкомата.
10. Следует сохранять распечатанные банкоматом квитанции для последующей сверки указанных в них сумм с выпиской по карточному счету.
11. Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций с банковской картой в банкоматах.
12. 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 - эмитент банковской карты (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

1. Не используйте банковские карты в организациях торговли и услуг, не вызывающих доверия.
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. При использовании банковской карты для оплаты товаров и услуг кассир может потребовать от владельца банковской карты предоставить паспорт (документ, удостоверяющий личность), 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.

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 карточному счету.

Рекомендации при совершении операций с банковской картой через сеть Интернет

1. Не используйте ПИН-код при заказе товаров и услуг через сеть Интернет, а также по телефону/факсу.
2. Не сообщайте персональные данные или информацию о банковской карте/карточном счете через сеть Интернет, например ПИН-код, пароли доступа к ресурсам банка, срок действия банковской карты, кредитные лимиты, историю операций.
3. С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с карточного 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.
4. Следует пользоваться интернет-сайтами только известных и проверенных организаций торговли и услуг.
5. 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.
6. Рекомендуется совершать покупки только со своего компьютера в целях сохранения конфиденциальности персональных данных и (или) информации о банковской карте/карточном 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).

7. 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.

Рекомендации при совершении операций с карточным токеном (для держателей карты «VISA»)

1. Устанавливайте программы, предназначенные для обнаружения вредоносных программ, поддерживающие соответствующий уровень безопасности на мобильном устройстве (антивирусное программное обеспечение), в том числе, предлагаемые провайдером.
2. Установите на мобильном устройстве блокировку экрана (блокировка входа в мобильное устройство).
3. Не оставляйте мобильное устройство без присмотра и (или) не передавайте его третьим лицам.
4. Не регистрируйте на мобильном устройстве средства аутентификации третьего лица.
5. Не храните личные данные, финансовую информацию и карточный токен на мобильном устройстве, использование которого прекращено, или при передаче мобильного устройства в организацию, осуществляющую ремонт техники.
6. Не блокируйте любые функции безопасности, предусмотренные на мобильном устройстве в целях защиты карточного токена.