Приложение №7 к Приказу
Председателя
Правления АО «Банк Акцепт»
от «06» сентября 2023 года № 680

ПАМЯТКА ПО ИСПОЛЬЗОВАНИЮ КАРТ

1. Для расчетов в сети Интернет рекомендуется установить лимит на совершение безналичных операций на сумму, меньше стандартных лимитов, устанавливаемых Банком по Картам. Изменить лимит на совершение безналичных операций или установить запрет на совершение таких операций Клиент может по письменному заявлению, оформленного в Банке или самостоятельно в Интернет-Банке (при наличии у Клиента).
2. Возможность совершения операций по Карте в сети Интернет (с использованием реквизитов карты) является доступной Клиенту сразу при выдачи карты Клиенту в Банке (при необходимости закрыть возможность совершения операций с использованием реквизитов карты в сети Интернет - Клиент может подать в БАНК соответствующее Заявление или самостоятельно установить запрет в системе Интернет-банк (при наличии у Клиента).
3. Для проведения операции в сети Интернет, как правило, используются следующие реквизиты Карты: номер карты, срок действия, имя и фамилия Держателя карты, указанные на карте, код безопасности CVV2/CVC2 — последние три цифры, указанные на полосе для подписи на оборотной стороне карты.
4. В целях дополнительного подтверждения совершаемой в сети Интернет операции (проверка принадлежности Карты лицу, совершающему операцию, по ее номеру) предусмотрено применение технологии безопасности для карты Verified by Visa («Проверено Visa»)/ МИР Accept (далее – «3d-Secure»), предусматривающей направление на номер мобильного телефона Клиента SMS-сообщения, содержащего одноразовый пароль, подлежащий введению в соответствующем диалоговом окне при совершении операции.
5. Сервис 3d-Secure подключается бесплатно при выдачи карты или содержится в сервисе «Информирование об операциях» (при подключении).
6. Запрещается сообщать через сеть Интернет (электронная почта, icq, skype и т.д.) такие данные как: ПИН, пароли доступа к ресурсам Банка, историю операций и иные персональные данные.
7. Обязательно убедитесь в правильности адресов интернет-сайтов, на которых собираетесь совершить покупки, т.к. похожие адреса могут быть использованы мошенниками для получения информации о Вашей Карте.
8. При расчетах в сети Интернет Держатель карты самостоятельно оценивает надежность торговой точки (срок работы, репутации, наличие почтового адреса и др.), для которой он указывает реквизиты своей Карты.
9. В целях безопасности, нельзя вводить данные Карты на сайтах, предлагающих «легкий» заработок в интернете, зачисление выигрышей и требующие для этого все реквизиты Карты и Персональные данные Держателя карты.
10. Перед оплатой покупки необходимо ознакомиться с условиями покупки, содержащимися на Интернет-сайте продавца: полным описанием товара, информацией о способах и стоимости доставки, дополнительными налогами, правилами предоставления услуг, процедурой возврата товара. Не производите оплату через Интернет-сайты в случае, если информация об условиях оплаты на них предоставлена на незнакомом Вам языке.
11. При получении от Банка SMS-сообщения на номер мобильного телефона Клиента и/или Push-уведомления с Разовым паролем следует внимательно ознакомиться с информацией в сообщении/уведомлении: все реквизиты операции в направленном Вам сообщении/уведомлении должны соответствовать той операции, которую Вы собираетесь совершить. Только после того, как Вы убедились, что информация в этом SMS-сообщении/Push-уведомлении корректна, можно вводить пароль для подтверждения операции. Помните, что, вводя Разовый пароль, Вы даёте Банку право и указание провести операцию по указанным в уведомлении (SMS-сообщении/Push-уведомлении) реквизитам. Запрещается сообщать свои пароли кому-либо, включая сотрудников Банка.

12. В случае осуществления Держателем Карты операций в сети Интернет с использованием реквизитов каких-либо эмитированных Банком Карт, Банк не гарантирует удовлетворение претензий по ним.
13. В случае возникновения спорной ситуации при оплате товара/услуги через сеть Интернет, следует сохранять любые электронные документы, переписку по электронной почте, касающуюся разрешения этой ситуации с организацией торговли (сервиса). При невозможности самостоятельно разрешить данную ситуацию нужно обратиться в Банк, предоставив вышеуказанную информацию.
14. Следует обращать внимание на информацию о дополнительных условиях, обычно представленную мелким шрифтом. Иногда, недобросовестные продавцы, предлагают проведение расчетов на основе ежемесячных или ежегодных платежей (например, за доставку товаров) до тех пор, пока Вы не пришлете сообщение о расторжении договора. Таким образом, предоставив данные своей Карты, Вы санкционируете ежемесячное/ежегодное списание определенной суммы и теряете право оспорить данные списания через Банк.
15. Необходимо совершать покупки только со своего личного компьютера/мобильного устройства в целях сохранения конфиденциальности персональных данных и(или) данных Карты. В случае если покупка совершается с чужого компьютера/мобильного устройства, не сохраняйте на нем персональные данные и данные Карты, а после завершения операций убедитесь, что эти данные не сохранились (заново открыв страницу интернет-сайта продавца, на которой совершались покупки).
16. Следует установить на свой компьютер/мобильное устройство современное антивирусное программное обеспечение и регулярно обновлять его, а так же другие программы, используемые Вами. Рекомендуется использовать только лицензионные программы, либо распространяемые свободно, полученные из надежных источников.
17. Перед тем как воспользоваться Банкоматом, осмотрите его на наличие дополнительных устройств, расположенных в месте набора ПИН (например, наличие неровно установленной клавиатуры или миниатюрной видеокамеры), в месте приема Карты и в месте выдачи купюр.
18. В случае если клавиатура, место для приема Карт или место выдачи купюр Банкомата оборудованы дополнительными устройствами, воздержитесь от использования Карты в данном Банкомате и сообщите о своих подозрениях сотрудникам Банка по телефону, указанному на банкомате.
19. Не применяйте физическую силу, для того чтобы вставить Карту в Банкомат. Если Карта не вставляется, воздержитесь от использования такого Банкомата.
20. Набирайте ПИН так, чтобы люди, находящиеся поблизости, не смогли его увидеть. (Например, прикрывайте клавиатуру рукой при вводе ПИН).
21. В случае если Банкомат работает некорректно (например, долгое время находится в режиме ожидания, самопроизвольно перезагружается), откажитесь от использования такого банкомата, отмените текущую операцию, нажав на клавиатуре кнопку «Отмена», и дождитесь возврата банковской карты. Воздержитесь от ввода ПИН в некорректно работающем Банкомате.
22. **При утере/краже Карты, рассекречивания ПИН-кода, утере/краже/порчи мобильного устройства (на котором установлено Мобильное приложение для использования Цифровой карты) во избежание возможности её использования третьими лицами, Клиенту/Держателю необходимо немедленно сообщить об этом в Банк/ Справочно-информационный Центр (также желательно заявить об этом в правоохранительные органы) для блокировки Карты:**
    а) Круглосуточно посредством мобильной связи с использованием сервиса «Информирование об операциях» (Тариф «Стандартный») (путем отправки SMS-команды на блокировку Карты) (при наличии подключенного сервиса).
    б) В рабочее время Контакт-центра Банка посредством телефонного звонка в Контакт-центр на номер телефона: +7-800-100-27-37. Сотрудник Контакт-центра идентифицирует по данным в программе по кодовому слову.
    в) Круглосуточно в Справочно-информационный Центр (ЗАО ПЦ «КартСтандарт») посредством телефонного звонка, указанного в Заявлении, на номер:
        – +7-800-200-45-75 (внутрироссийский звонок);
        – +7(383) 363-11-58 (трансграничный звонок).

        При этом не позднее рабочего дня, следующего за обращением в круглосуточный Справочно-информационный Центр, необходимо обратиться по телефону в Банк, для блокировки Карты в автоматизированной банковской системе.
    г) Заблокировать Карту самостоятельно через систему Интернет-Банк (при наличии у Клиента).