ТАВРИЧЕСКИЙ БАНК

Таврический Банк
(акционерное общество)
191123, Россия, Санкт-Петербург,
ул. Радищева, д. 39

Памятка Клиента
по мерам безопасности использования карт и сервисов Таврического Банка (АО)

Санкт-Петербург
2019

Содержание

Соблюдение рекомендаций, содержащихся в Памятке, позволит обеспечить максимальную сохранность вашей банковской карты, ее реквизитов, ПИН-кода и других данных, а также позволит снизить возможные риски при совершении операций с использованием банковской карты.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Телефоны клиентской поддержки Таврического Банка (АО) 8(800)700-45-93 (круглосуточно), 8(812)329-55-12 указаны на оборотной стороне банковской карты и на веб-сайте Банка www.tavrich.ru. Этот телефон необходимо иметь при себе на других носителях информации: в записной книжке, мобильном телефоне и/или других носителях информации, но не рядом с записью о ПИН-коде.
Срок действия карты указан на лицевой стороне карты.

1.2. По истечении срока действия карта (ее реквизиты) не действительна/ы.

1.3. Держателем карты является лицо, имя которого указано на лицевой стороне карты (в случае если присутствует) и образец подписи которого имеется на ее оборотной стороне, получившее от банка право на пользование картой.

1.4. Карта предназначена для проведения операций в торговых и сервисных точках, в банковских учреждениях и банкоматах, на которых размещены логотипы (товарные знаки) соответствующих платежных систем.

2. РЕКОМЕНДАЦИИ О МЕРАХ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ КАРТ

2.1. Храните в секрете ПИН-код, срок действия карты, код CVC/CVV-код (трехзначный код, расположенный на обратной стороне банковской карты, на полосе для подписи).

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

2.3. 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.

2.4. 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.

2.5. 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.

2.6. 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.

2.7. С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковского счета целесообразно установить лимит, ограничивающий сумму или количество операций по банковской карте и одновременно подключить услугу оповещения о проведенных операциях (например, оповещение посредством СМС-сообщений или PUSH -уведомлений).

2.8. При получении просьбы, в том числе со стороны сотрудника банка, сообщить персональные данные или информацию о банковской карте (в том числе ПИН-код, CVC/CVV-код, код из СМС-сообщения или PUSH –уведомления от банка) не сообщайте их. Немедленно перезвоните по телефону клиентской поддержки Таврического Банка 8(800)700-45-93 (круглосуточно), 8(812)329-55-12 и сообщите о данном факте.

2.9. 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.

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

2.11. В случае, если имеются предположения о раскрытии ПИН-кода, персональных данных, позволяющих совершить неправомерные действия с вашим банковским счетом, а также если банковская карта была утрачена, необходимо немедленно обратиться в банк и следовать указаниям сотрудника.

2.12. До момента обращения в банк вы несете риск, связанный с несанкционированным списанием денежных средств с вашего банковского счета. Согласно условиям договора с банком денежные средства, списанные с вашего банковского счета в результате несанкционированного использования вашей банковской карты до момента уведомления об этом банка, не возмещаются.

2.13. Не оставляйте свой смартфон без присмотра, чтобы исключить несанкционированное использование мобильных банковских услуг. Установите на смартфоне пароль, данная возможность доступна для любых современных моделей смартфонов.

2.14. Установите на смартфон антивирусное ПО и своевременно его обновляйте.

2.15. При внезапном прекращении работы SIM-карты необходимо обратиться к оператору сотовой связи за уточнением причин – в отношении вас возможно проведение мошеннических действий третьими лицами.

2.16. Не переходите по ссылкам и не устанавливайте приложения или обновления безопасности, пришедшие по СМС или электронной почте, в том числе от имени банка.

3. РЕКОМЕНДАЦИИ О МЕРАХ БЕЗОПАСНОСТИ ПРИ СОВЕРШЕНИИ ОПЕРАЦИЙ С КАРТОЙ В БАНКОМАТАХ

3.1. Осуществляйте операции с использованием банкоматов, установленных в безопасных местах (например, в государственных учреждениях, подразделениях банков, крупных торговых комплексах, гостиницах, аэропортах и т.п.).

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

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

3.4. 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 банка по телефону, указанному на банкомате.

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

3.6. До набора ПИН-кода нажмите на клавиатуре кнопку «Отмена» с целью избежания списания средств мошенническим путем.

3.7. Набирайте ПИН-код таким образом, чтобы люди, находящиеся в непосредственной близости, не смогли его увидеть.
3.8. При наборе ПИН-кода прикрывайте клавиатуру рукой.
3.9. 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.
3.10. 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.
3.11. Следует сохранять распечатанные банкоматом квитанции для последующей сверки указанных в них сумм с выпиской по банковскому счету.
3.12. Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций с банковской картой в банкоматах.
3.13. Не производите операций в банкомате, следуя инструкциям посторонних лиц, в том числе выдаваемых вам удаленно по мобильному телефону.
3.14. 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 банк и заблокировать карту.

4. РЕКОМЕНДАЦИИ ПРИ ИСПОЛЬЗОВАНИИ КАРТЫ ДЛЯ БЕЗНАЛИЧНОЙ ОПЛАТЫ ТОВАРОВ И УСЛУГ

4.1. Не используйте банковские карты в организациях торговли и услуг, не вызывающих доверия.
4.2. 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.
4.3. 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. Проверяйте сумму операции перед тем как подписать чек, набрать ПИН-код.
4.4. 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.

5. РЕКОМЕНДАЦИИ ПРИ СОВЕРШЕНИИ ОПЕРАЦИЙ С КАРТОЙ В ИНТЕРНЕТ-МАГАЗИНАХ

5.1. Не используйте ПИН-код при заказе товаров и услуг через сеть Интернет, а также по телефону/факсу.
5.2. Не сообщайте персональные данные или информацию о банковской(ом) карте (счете) через сеть Интернет, например, ПИН-код, CVC/CVV-код, пароли доступа к ресурсам Банка, одноразовые пороли, направляемые банком в виде СМС-сообщений PUSH-уведомлений на ваш номер телефона для проведения операций, срок действия банковской карты, кредитные лимиты, историю операций, персональные данные.

5.3. 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 с предельным лимитом, предназначенным только для указанной цели. Для безопасного проведения операций в сети Интернет необходимо подключить сервис получения СМС-сообщений по технологии 3-D Secure, содержащих код для совершения операций.

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

5.5. 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.

5.6. 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).

5.7. 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.