ПАМЯТКА ПО БЕЗОПАСНОМУ ИСПОЛЬЗОВАНИЮ БАНКОВСКИХ КАРТ

Уважаемый Держатель банковской карты!

Убедительно просим Вас внимательно ознакомиться и в дальнейшем следовать требованиям безопасности, изложенным в настоящей Памятке.

Банковская карта является электронным средством платежа, защищенным от подделки и несанкционированного использования третьими лицами.

Платежные системы постоянно работают над усовершенствованием средств защиты банковских карт, но гарантировать, что злоумышленники не смогут похитить вашу карту (скопировать ее) и таким образом совершить операции, наносящие вам материальный ущерб, не может никто.

ПОМНИТЕ, ЧТО СНИЖЕНИЕ РИСКА ТАКОГО УЩЕРБА В ПЕРВУЮ ОЧЕРЕДЬ ЗАВИСИТ ОТ ВАШЕЙ СОБСТВЕННОЙ ОСМОТРИТЕЛЬНОСТИ!

1. ОБЩИЕ ПРАВИЛА БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ КАРТЫ

1.1. Никогда и никому не сообщайте ПИН-код банковской карты, в том числе: родственникам, знакомым, сотрудникам кредитных организаций, кассирам и лицам, помогающим Вам в использовании банковской карты. ПИН-код набирается исключительно на клавиатуре банкомата или платежного терминала;

1.2. ПИН-код является аналогом Вашей подписи и его необходимо запомнить. В случае если это для Вас затруднительно, храните его отдельно от банковской карты, желательно в неявном виде и в недоступном для третьих лиц (включая ваших родственников) месте;

1.3. Никогда ни при каких обстоятельствах не передавайте банковскую карту для использования третьим лицам, в том числе вашим родственникам. Право использовать банковскую карту имеет только то физическое лицо, фамилия и имя которого указаны на банковской карте;

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

1.5. Обязательно подключите Услугу «SMS-информирование» об операциях по банковской карте. Это поможет вам незамедлительно заблокировать банковскую карту в случае несанкционированных операций по ней и уменьшить размер ущерба;

1.6. Не забудьте о возможности установить суточный лимит на сумму операций по банковской карте. Это поможет вам уменьшить размер ущерба в случае несанкционированных операций по банковской карте;

1.7. Не забудьте о возможности установить территориальные ограничения на совершение операций по банковской карте. Например, когда вы находитесь в пределах Российской Федерации, вы можете запретить проведение операций по банковской карте во всех странах, кроме РФ. Такой запрет ограничит злоумышленников в их мошеннических действиях и поможет вам предотвратить ущерб;

1.8. Для снижения риска проведения мошеннических операций по карте рекомендуется определить для карты список стран, в которых собираетесь использовать карту. Все запросы на проведение операций по карте, поступающие из стран, отличных от разрешенных Держателем, будут отклоняться. Установить/ отменить данные ограничения использования карты, а также изменить список разрешенных стран можно при телефонном обращении в банковских карт ББР Банк (АО);

1.9. Не отвечайте на электронные письма, в которых от имени ББР Банка (АО) предлагается предоставить персональные данные. Не следуйте по ссылкам, указанным в электронных письмах (включая ссылки на сайт ББР Банк (АО), т.к. они могут вести на «интернет-сайты - двойники». Банк НИКОГДА не просит подойти к банкомату и ввести т.н. «коды разблокировки».

1.10. Для информационного взаимодействия с ББР Банком (АО) используйте только те 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 ББР Банке (АО);

1.11. В случае раскрытия ПИН-кода, персональных данных, утраты банковской карты либо предположения о таком раскрытии или утрате, немедленно обратитесь в ББР Банк (АО) и следуйте указаниям сотрудника.

2. МЕРЫ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ КАРТЫ ДЛЯ БЕЗНАЛИЧНОЙ ОПЛАТЫ ТОВАРОВ И УСЛУГ

2.1. Не выпускайте вашу банковскую карту из поля зрения; требуйте, чтобы операции с банковской картой проводились в вашем присутствии (с использованием переносных терминалов

либо в вашем присутствии в кассе). Такие действия снизят риск копирования банковский карты и получения Ваших персональных данных, указанных на банковской карте;

2.2. Не используйте банковские карты в организациях торговли и услуг, не вызывающих вашего доверия;

2.3. Предъявляйте кассиру по его требованию документ, удостоверяющий вашу личность. Отнеситесь к этому с пониманием - такие меры помогают защитить вас от действий мошенников;

2.4. Перед набором ПИН-кода убедитесь, что люди, находящиеся в непосредственной близости, не смогут его увидеть. Перед тем, как подписать чек, в обязательном порядке проверьте сумму, указанную на чеке;

2.5. В случае «неуспешной» операции сохраните один экземпляр выданного терминалом чека для последующей проверки на отсутствие указанной операции в выписке по банковскому счету.

3. МЕРЫ БЕЗОПАСНОСТИ ПРИ СОВЕРШЕНИИ ОПЕРАЦИЙ С ИСПОЛЬЗОВАНИЕМ КАРТЫ В БАНКОМАТЕ

3.1. Старайтесь осуществлять операции только в банкоматах, установленных в охраняемых помещениях (например, в государственных учреждениях, подразделениях банков, крупных торговых комплексах, гостиницах, аэропортах и т.п.);

3.2. Никогда не вводите ПИН–код для доступа в помещение, где расположен банкомат;

3.3. В случае если поблизости от банкомата находятся посторонние лица, выберите другое время или другой банкомат для совершения операции;

3.4. Не забывайте внимательно посмотреть на банкомат (на экран, клавиатуру, прорезь для приема/выдачи банковской карты) перед совершением каждой операции. Если ваше внимание привлек необычный вид этих частей банкомата (например, в них установлены дополнительные устройства, неровно установлена клавиатура), - воздержитесь от использования такого банкомата; о своих подозрениях сообщите в кредитную организацию 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. Не набирайте ПИН-код таким образом, чтобы люди, находящиеся в непосредственной близости, не смогли его увидеть. При наборе ПИН-кода прикрывайте клавиатуру рукой;

3.7. 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;

3.8. После получения наличных денежных средств в банкомате, пересчитайте банкноты полистно, убедитесь в том, что банковская карта возвращена банкоматом, дождитесь выдачи квитанции при ее запросе, затем положите их в сумку (кошелек, карман) и только после этого отходите от банкомата;

3.9. Сохраняйте распечатанные банкоматом квитанции для последующей сверки указанных в них сумм с выпиской по банковскому счету;

3.10. Не принимайте советы и помощь третьих лиц при проведении операций с банковской картой в банкоматах;

3.11. Если при проведении операций с банковской картой банкомат не возвращает банковскую карту, позвоните в кредитную организацию по телефону, указанному на банкомате, объясните обстоятельства произошедшего, а также обратитесь в ББР Банк (АО), и далее следуйте инструкциям сотрудника.

4. МЕРЫ БЕЗОПАСНОСТИ ПРИ СОВЕРШЕНИИ ОПЕРАЦИЙ С ИСПОЛЬЗОВАНИЕМ РЕКВИЗИТОВ КАРТ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ»

4.1. ПИН-код **НИКОГДА НЕ ИСПОЛЬЗУЕТСЯ** при заказе товаров и услуг через сеть Интернет;

4.2. Никогда не сообщайте никакие персональные данные, за исключением указанных на банковской карте;

4.3. Не забывайте о возможности использовать отдельную банковскую карту, с ограниченным кругом операций - только для покупок в сети Интернет. Это позволит вам уменьшить размер ущерба от возможных мошеннических действий;

4.4. Для покупок пользуйтесь интернет-сайтами только известных и проверенных торговых организаций;

4.5. Для проведения операций в сети Интернет требуются данные: номер карты, срок действия, имя и фамилия Держателя, код безопасности – CVV2/ CVC2/ ППК2. Код безопасности указан на оборотной стороне карты;

4.6. Обращайте внимание на наличие логотипов MirAccept, Verified by Visa или Mastercard SecureCode на интернет-сайтах. Операции оплаты на таких сайтах дополнительно защищены современным протоколом безопасности 3D-Secure, для подтверждения таких операций Вы будете перенаправлены на сайт банка, где должны будете ввести код подтверждения, отправленный Вам на мобильный телефон;

4.7. Код подтверждения при осуществлении On-Line покупок или при переводах денежных средств НИКОГДА НИКОМУ НЕ ТРЕБУЕТСЯ ПЕРЕСЫЛАТЬ или СООБЩАТЬ;

4.8. Обязательно убедитесь в правильности адресов web-сайтов, к которым вы подключаетесь, и на которых собираетесь совершить покупки. Похожие адреса могут использоваться для осуществления мошеннических действий;
4.9. Совершайте покупки только со своего личного компьютера в целях сохранения конфиденциальности персональных данных и информации о банковской карте (счете);
4.10. В случае если все же покупка совершается с использованием чужого компьютера, не сохраняйте на нем ваши персональные данные и другую информацию. После завершения всех операций убедитесь, что персональные данные и другая информация не сохранилась (вновь загрузите в браузере web-страницу продавца, на которой совершались покупки);
4.11. Не совершайте покупок с компьютера, на котором не установлено антивирусное программное обеспечение.

5. ДОПОЛНИТЕЛЬНЫЙ КОНТРОЛЬ, СВЯЗАННЫЙ С РАБОТОЙ СЕРВИСА «МГНОВЕННЫЕ ПЕРЕВОДЫ С КАРТЫ НА КАРТУ ОНЛАЙН» НА САЙТЕ БАНКА.

5.1. Убедитесь, что перевод денежных средств с карты на карту осуществляете на правильной web-странице Банка (https://bbr.ru) или в Мобильном приложении Банка «ББР Онлайн».
5.2. Обращаем Ваше внимание, что валюта перевода денежных средств - рубли Российской Федерации.
5.3. После ручного ввода параметров перевода, а именно:

- номер Карты плательщика;
- срок действия Карты плательщика;
- адрес электронной почты плательщика
- номер Карты получателя;
- сумму перевода в рублях Российской Федерации -

осуществить дополнительную проверку параметров перевода, в том числе корректность указания номеров Карт плательщика и получателя, суммы перевода и расчета комиссии.

Обращайте внимание на правильность адреса web-страницы Банка (https://bbr.ru), с которой осуществляете ввод одноразового пароля - протокол безопасности 3D-Secure, т.к. похожие адреса могут использоваться третьими лицами для осуществления неправомерных действий с Вашими банковскими картами. Банк направляет SMS-сообщение с одноразовым паролем на номер мобильного телефона, указанный при подключении карты к Услуге «SMS-информирование» / «3D-Secure». Подтверждение перевода осуществляется вводом одноразового пароля на специальной web-странице Банка, сначала, сверху страницы указан логотип Платежной системы Вашей банковской карты, далее размещен логотип Банка.

или


или


Обязательно, проверьте, что:

- Интернет-Магазин – Best2Pay Transfer;
- Сумма платежа – указана Вами верно!

5.4. Не осуществляйте перевод денежных средств на одном устройстве одновременно в нескольких открытых приложениях; необходимо предусмотреть возможность проведения операции по переводу денежных средств и получение одноразового пароля от Банка на разных устройствах.
5.5. Проверьте, если перевод выполнен успешно, уведомление по операции поступит на Ваш адрес электронной почты, указанной при вводе параметром перевода от *noreply@best2pay.net* с ссылкой на ББР Банк (АО).
5.6. В случае введения плательщиком **некорректных реквизитов** при вводе параметров на перевод денежных средств, в результате чего перевод может быть выполнен в пользу иного лица, возврат средств по осуществленному переводу возможен только по личному распоряжению получателя либо по решению судебных органов.