ПРАВИЛА
пользования банковской картой ПАО Банк «Кузнецкий»

Требования по соблюдению мер безопасности, содержащихся в настоящих Правилах, являются обязательными и направлены на предотвращение возникновения финансовых потерь у держателя банковской карты (далее - Клиент) в результате совершения противоправных действий с использованием карты. В случае нарушений Клиентом настоящих Правил пользования картой, например, при разглашении ПИН-кода, реквизитов карты, персональных данных Клиента, а также в случае утраты карты, карта становится источником повышенного риска несанкционированного списания денежных средств с карточного счета Клиента. В результате нарушения Правил, неправомерно полученные сведения о реквизитах карты могут быть использованы мошенниками для совершения несанкционированных Клиентом операций, для изготовления поддельных карт, частично или полностью имитирующих подлинные, следствием чего являются финансовые потери Клиента.

1. Общие правила безопасности

1.1. При получении новой карты Клиент обязан проставить свою подпись на оборотной стороне карты на полосе для подписи.

1.2. Клиент обязан хранить в секрете ПИН-код (персональный идентификационный номер) и реквизиты карты (номер карты, срок действия, трехзначный код проверки действительности карты, указанный на оборотной стороне карты), одноразовые пароли, направляемые Банком на номер мобильного телефона Клиента в целях дополнительной идентификации при совершении операций с использованием реквизитов карты в сети Интернет. Клиент никогда не должен сообщать ПИН-код третьим лицам, в том числе родственникам, знакомым, сотрудникам банков, кассирам и лицам, помогающим ему в использовании карты. Запрещается записывать ПИН-код на карте и хранить его рядом с картой. Запрещается записывать ПИН-код в память мобильного телефона без его шифрования или без установления соответствующей блокировки телефона. Несоблюдение данного правила приводит к тому, что по карте, похищенной вместе с телефоном, содержащим сведения о ПИН-коде, мошенники получают полный доступ к денежным средствам Клиента.

1.3. Передача карты для использования третьим лицам, в том числе родственникам является нарушением Правил пользования картой. По желанию Клиента Банком может быть выпущена дополнительная карта к карточному счету Клиента. Использовать карту имеет право только лицо, имя которого указано на карте.

1.4. Запрещается предоставлять посторонним лицам сведения о своих персональных данных, реквизитах карты и (или) ПИН-коде, одноразовых паролях в ответах на электронные письма, СМС-сообщения или звонки, в которых от имени Банка предлагается предоставить такие данные. В случае сомнений, что звонок или сообщение исходят из Банка, следует самостоятельно перезвонить по телефону, указанному на обороте карты в Единую службу поддержки держателей карт Банка.

1.5. В случае поступления мошеннических СМС-сообщений / Push-уведомлений / рассылки по электронной почте или звонка третьих лиц, представившихся работниками Банка (например, службы безопасности, службы технической поддержки и т.п.), побуждающих незамедлительно провести действия с Картой (например, по разблокировке карты, отмене перевода денежных средств и т.п.) путем сообщения конфиденциальной информации (ПИН-код, Реквизиты Карты), Клиенту запрещается:

- предоставлять запрашиваемую информацию;
- проводить любые действия / операции с Картой по инструкциям, полученным указанными способами.

Клиенту следует незамедлительно:

- прервать общение с мошенниками (завершить телефонный разговор, не отвечать на СМС-сообщения / Push-уведомления / e-mailрассылку);
- уведомить Банк о случившемся.

1.6. В целях информационного взаимодействия с Банком следует использовать только реквизиты средств связи (мобильных и стационарных телефонов, факсов, интерактивных интернет-сайтов, обычной и электронной почты и пр.), которые указаны в документах, полученных непосредственно в Банке.

1.7. Клиент обязан проверять выписку по карточному счету, в которой указываются операции за отчетный период, не реже одного раза в месяц. В случае обнаружения подозрительных или неизвестных операций Клиент обязан немедленно сообщить об этом в Банк. Банк также предоставляет Клиенту возможность оперативно получить информацию об остатке денежных средств на своем карточном счете, а также об операциях, совершенных по карточному счету, путем обращения в Единую службу поддержки клиентов.

1.8. Для дополнительной безопасности и незамедлительного получения информации об операциях, совершенных с использованием карты (реквизитов карты), Банк предоставляет возможность и настоятельно рекомендует Клиенту подключать услугу СМС-информирования.

1.9. Банк предоставляет Клиенту возможность и право установить индивидуальные значения лимитов безопасности на проведение операций с использованием карт по его заявлению при личном обращении в Банк. Установление Клиентом повышенных индивидуальных значений лимитов безопасности несет повышенный риск финансовых потерь Клиента в случае несанкционированного использования карты посторонними лицами и иных мошеннических операций.

1.10. В случае утраты (кражи) карты и (или) ПИН-кода, а также в случае риска возникновения несанкционированного использования карты, ее реквизитов и (или) ПИН-кода, Клиент обязан незамедлительно уведомить об этом Банк по телефонам 8-495-924-75-00, 8-383-363-11-58, 8-800-100-64-10, (8412) 23-18-72, 23-18-25, а также в течение трех рабочих дней обратиться в офис Банка с письменным заявлением об обнаружении факта утраты банковской карты и(или) использования её реквизитов без согласия Клиента.

1.11. Банк имеет право приостановить или полностью прекратить действие карты в случае возникновения подозрений в компрометации карты, при возможном мошенничестве с использованием карты, реквизитов карты. Действие карты может быть восстановлено при устранении причин приостановки ее действия.

1.12. В целях предотвращения возникновения финансовых потерь у Клиента при наборе неверного ПИН-кода три раза подряд действие карты приостанавливается (блокируется). Разблокировать карту держатель карты может обратившись по телефонам 8-495-924-75-00, 8-383-363-11-58, 8-800-100-64-10, (8412) 23-18-72, 23-18-25, а также обратившись подразделение Банка.

2. Правила безопасности при совершении операций с картой в банкомате

2.1. До совершения операции следует обратить внимание на внешний вид банкомата. Запрещается совершать операции при обнаружении любых внешних признаков неисправности банкомата или обнаружении рядом с ним или на нем посторонних устройств, накладных панелей, инородных предметов в (на) картоприемнике, клавиатуре банкомата, отверстии для выдачи наличных. При обнаружении посторонних устройств и предметов следует сообщить об этом в банк по телефону, указанному на банкомате, и воспользоваться другим банкоматом.

2.2. Если Карта не вставляется в банкомат, запрещается применять физическую силу чтобы вставить карту, следует воздержаться от использования такого банкомата.

2.3. Не следует использовать устройства, которые требуют ввода ПИН-кода для доступа в помещение, где расположен банкомат. Следует избегать использования банкоматов в плохо освещенных и безлюдных местах.

2.4. 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 карты.

2.5. Не допускайте присутствия сторонних лиц при проведении операции. При наличии установленных на банкомате специальных зеркал наблюдения воспользуйтесь ими для снижения риска несанкционированного наблюдения третьими лицами за проведением Вами операции. Следует убедиться в том, что люди, стоящие рядом с Вами, не имеют возможности увидеть ПИН-код или сумму снимаемых наличных. При наборе ПИН-кода на банкоматах, не оборудованных закрывающей клавиатуру защитной шторкой, прикрывайте клавиатуру рукой.

2.6. При совершении операций с картой запрещается руководствоваться советами третьих лиц. В случае возникновения каких-либо проблем при совершении операции (например, банкомат не возвращает карту) следует незамедлительно обратиться в Банк по номерам телефонов Единой службы поддержки клиентов, объяснить обстоятельства произошедшего и следовать инструкциям сотрудника Банка.

2.7. Если банкомат стороннего банка не возвращает карту, то Клиенту следует:

- по телефону, указанному на банкомате, обратиться в банк - владелец банкомата и выяснить сроки и порядок возврата карты;
- заблокировать карту, т. к. карта, находящаяся не на руках ее держателя, не должна быть активной.

2.8. При проведении операции не следует отходить от банкомата. Возвращенную банкоматом карту следует немедленно убрать в сумку (кошелек, карман), полученные наличные денежные средства пересчитать полистно, убрать их, дождаться выдачи квитанции при ее запросе, и только после этого отходить от банкомата.

2.9. Не проводите действий в банкоматах по инструкциям, полученным по телефону. Всегда уточняйте полученную информацию только по телефонам, указанным на оборотной стороне карты или по телефону службы технической поддержки, указанному на Сайте Банка.

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

3. Правила безопасности при использовании карты для безналичной оплаты товаров и услуг

3.1. Клиент обязан требовать проведения операций с его картой только в своем присутствии. Это необходимо в целях снижения риска неправомерного получения персональных данных, указанных на карте, и реквизитов карты.

3.2. При оплате товаров и услуг с использованием карты кассир может потребовать от владельца карты подписать чек и (или) ввести ПИН-код, предъявить документ, удостоверяющий личность. При наборе ПИН-кода следует прикрывать клавиатуру рукой. Перед подписанием чека следует обязательно проверить сумму, указанную на чеке, а при получении СМС-сообщения (в случае подключения соответствующей услуги), информирующего о совершенной операции, проверить сумму фактического списания с карточного счета.

3.3. Не используйте карту в организациях торговли и услуг, если торговая точка и (или) ее персонал не вызывают у Вас доверия.

3.4. В случае если при попытке оплаты картой имела место «неуспешная» операция, следует сохранять выданный терминалом чек, свидетельствующий о неуспешном завершении операции, для последующей проверки отсутствия указанной операции в выписке по карточному счету.

3.5. В зависимости от технологии оплаты и настроек POS-терминала торговой точки операции безналичной оплаты товаров и услуг с использованием карты могут проводиться без подтверждения (без ввода ПИН-кода и без проставления подписи держателя карты в документе, составленном при совершении операции) в рамках установленных Банком значений лимитов безопасности. Клиентом могут быть установлены индивидуальные значения лимитов безопасности на проведение указанных операций, при этом при установлении повышенных значений Клиент несет повышенный риск финансовых потерь в случае несанкционированного использования карты посторонними лицами, в случае иных мошеннических операций. В целях предотвращения возникновения финансовых потерь у Клиента при проведении операций без подтверждения Банк рекомендует Клиенту установить индивидуальные значения лимитов безопасности с нулевыми значениями.

4. Правила безопасности при совершении операций по карточному счету через сеть Интернет

4.1. При совершении операций по карточному счету через сеть Интернет существует риск получения мошенниками персональных данных Клиента (в том числе паролей, реквизитов карты и карточного счета. С целью снижения таких рисков запрещается:

- следовать по ссылкам, указанным в подобных электронных письмах (включая ссылки на сайт Банка), т. к. они могут вести на сайты-двойники;
- сообщать ПИН-код через сеть Интернет;
- сообщать свои персональные данные или информацию о карте (карточном счете) через сеть Интернет, например, пароли доступа к ресурсам Банка, кредитные лимиты, историю операций, персональные данные;
- совершать покупки с чужого компьютера. Клиент обязан установить на свой компьютер антивирусное программное обеспечение и регулярно производить его обновление и обновление других используемых программных продуктов (операционной системы и прикладных программ).

4.2. Клиент обязан настроить операционную систему на своем компьютере так, чтобы обеспечивались основные правила безопасности работы в сети и соблюдались рекомендации Банка по безопасному совершению операций с банковской картой.

4.3. С целью минимизации рисков, связанных с проведением неправомерных операций по карточному счету, для оплаты покупок в сети Интернет Банк предоставляет возможность и настоятельно рекомендует:

- либо использовать карту с отдельным карточным счетом, открытую только для осуществления покупок в сети Интернет, и не размещать на таком карточном счете денежные средства в сумме, значительно превышающей сумму предполагаемой операции;
- либо оформить дополнительную карту к своему карточному счету и установить по такой карте индивидуальные значения лимитов безопасности на проведение операций.

4.4. Для совершения покупок через Интернет Клиент обязан пользоваться защищенной версией протокола HTTP браузера. Буква «s» после «http» в строке интернет-адреса означает, что Ваш браузер работает в безопасном режиме, при этом используется протокол SSL, что предотвращает перехват информации, переданной Вами по каналам Интернета.

4.5. При осуществлении покупок Клиент обязан пользоваться Интернет сайтами только известных и проверенных организаций торговли и услуг.

4.6. Клиент обязан убедиться в правильности адреса Интернет сайта, к которому подключается и на котором собирается совершить покупки, т.к. похожие адреса могут использоваться для осуществления неправомерных действий.

4.7. Перед совершением покупки Клиент обязан узнать больше информации об Интернет-магазине:

- прочитать опубликованные на сайте правила работы с информацией личного характера. Обратить внимание на меры обеспечения Интернет-магазином информационной безопасности;
- убедиться в том, что Интернет-магазин использует подтвержденный сертификат для обеспечения информационной безопасности. Желательно подтверждение сертификата подлинности одним из всемирных доверенных сертификационных агентств, например, http://www.verisign.com/ или http://www.globalsign.com/;

- убедиться в наличии у Интернет-магазина фактического адреса и зарегистрированного юридического лица, эти данные должны быть указаны на сайте;
- ознакомиться с условиями поставки товара и правилами его возврата, правилами предоставления услуги, в том числе о дополнительных сборах;
- проверить, есть ли на сайте Интернет-магазина форум, где посетители оставляют отзывы. Ознакомиться с отзывами о магазине на иных сайтах сети Интернет.

4.8. Клиент обязан сохранять конфиденциальность своего пароля и периодически менять его. Запрещается сохранять в системе пароли и сообщать свои пароли, используемые для входа на сайт Интернет-магазина, третьим лицам. Банк рекомендует не использовать просто вычисляемые пароли (например, дата рождения, номера телефона), а также использовать одинаковый пароль для Интернетмагазинов, своей почты и других систем.

4.9. При совершении покупок через Интернет не отказывайтесь от чека. Помните, что магазин обязан выдать Вам чек. Электронный чек приравнивается к бумажному, имеет юридическую силу и является полноценным документом, подтверждающим совершение покупки.