ПРАВИЛА ПОЛЬЗОВАНИЯ КАРТОЙ

Требования по соблюдению мер безопасности, содержащихся в Правилах пользования Картой, являются обязательными и направлены на предотвращение возникновения финансовых потерь у Держателя Карты в результате совершения противоправных действий с использованием Карты. В случае нарушений Клиентом 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 пользования Картой, 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 (за исключением Карты-браслета).

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, либо предоставленный Клиенту в Системе «Интернет-Банк» при оформлении Виртуальной Карты либо предоставленные Клиенту в ПИН-конверте при выдаче Карты-браслета), одноразовые пароли, направляемые Банком на Номер мобильного телефона / в Мобильное приложение 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. Если необходимо, для доверенных лиц Клиента может быть выпущена Дополнительная Карта. Использовать Карту имеет право только лицо, имя которого указано на Карте (за исключением Неэмбоссированной Карты и Карты-браслета, имя и фамилия держателя на которых не указываются).

1.4. Запрещается предоставлять посторонним лицам сведения о своих персональных данных, Реквизитах Карты и (или) ПИН-коде, одноразовых паролях в ответах на электронные письма, sms-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 клиентов.

1.5. В случае поступления мошеннических sms-сообщений / Push-уведомлений / рассылки по электронной почте / сообщений в социальных сетях / мессенджерах / интернет-сервисах или звонка третьих лиц, в том числе представившихся работниками Банка (например, службы безопасности, службы технической поддержки и т.п.), побуждающих незамедлительно провести действия с Картой / Мобильным приложением (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;
- устанавливать приложения по инструкциям, полученным указанным способом.

Клиенту следует незамедлительно:

- прервать общение с мошенниками (завершить телефонный разговор, не отвечать на sms-сообщения / Push-уведомления / e-mail-рассылку / сообщения в социальных сетях / мессенджерах / интернет-сервисах);
- 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.), указанных в документах, полученных непосредственно в Банке, либо размещенных на Сайте Банка.

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 системы «SMS-сервис» ABR-INFO.

1.9. Банк предоставляет Клиенту возможность и право установить индивидуальные значения лимитов безопасности на проведение операций с использованием Карт по его заявлению Клиента при личном обращении в Банк, в Системе «Интернет-Банк» (если с Клиентом заключен соответствующий договор) или при обращении в Единую службу поддержки клиентов по одному из номеров телефонов, указанных на Сайте Банка. Информация о размере и видах устанавливаемых Банком лимитов безопасности размещается на официальном сайте Банка в сети Интернет по адресу www.abr.ru. 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 одним из следующих способов:

- по номерам телефонов, указанным на обратной стороне Карты;
- по одному из номеров телефонов Единой службы поддержки клиентов, указанных на Сайте Банка:

  8 800 5003322, 8 800 1001111 (круглосуточно, звонок по России бесплатный)
  +7 495 7211001, +7 812 3353322 (круглосуточно, звонок платный);
- при личном обращении в Банк.

Необходимо всегда иметь при себе контактные телефоны Банка. До момента обращения в Банк Клиент несет риск, связанный с несанкционированным списанием денежных средств с Карточного счета.

1.11. В случае совершения противоправных действий против Клиента с целью завладения Картой, ПИН-кодом, Реквизитами Карты, Клиенту следует незамедлительно обратиться в ближайший отдел полиции.

1.12. Клиент обязан внимательно относиться к условиям хранения и использования Карты, предотвращать механическое, температурное и электромагнитное воздействие на Карту, избегать попадания на нее влаги. Запрещается хранить Карту рядом с мобильным телефоном, бытовой и офисной техникой.

1.13. Банк имеет право приостановить или полностью прекратить действие Карты в случае возникновения подозрений в Компрометации Карты, восстановить действие Карты при устранении причин приостановки ее действия, а также уведомить Клиента в течение 1 (одного) дня с момента приостановления (прекращения) действия Карты по инициативе Банка одним из следующих способов:

- путем уведомления по любому номеру телефона, предоставленному Клиентом Банку;
- путем направления sms-сообщения по Номеру мобильного телефона;
- путем направления уведомления по адресу электронной почты, предоставленному Клиентом Банку;
- путем направления письменного уведомления заказным письмом;
- уведомлением, направленным по Системе «Интернет-Банк» (если с Клиентом заключен соответствующий договор).

1.14. В целях предотвращения возникновения финансовых потерь у Клиента при наборе неверного ПИН-кода три раза подряд действие Карты приостанавливается (блокируется). Разблокировать Карту Держатель может одним из следующих способов:

- по номерам телефонов Единой службы поддержки клиентов, указанных на официальном сайте Банка в сети Интернет по адресу www.abr.ru;
- обратившись в любое 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 использовать банкоматы, установленные в безопасных местах (например, в государственных учреждениях, подразделениях банков, крупных торговых комплексах, гостиницах, аэропортах и т.п.). 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 работника 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;
- по телефону Единой службы поддержки клиентов заблокировать Карту, так как Карта, находящаяся не на руках ее Держателя, не должна быть активной.

2.8. При проведении операции не следует отходить от банкомата. Возвращённую 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 совершении операций с Картой в торгово-сервисных предприятиях

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 использовании Карты для оплаты товаров и услуг кассир может потребовать от Держателя 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 sms-сообщения/Push-уведомления, информирующего о совершённой операции, проверить сумму фактического списания с Карточного счёта.

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 совершения операции с 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.

При совершении операции снятия наличных денежных средств в POS-терминале одновременно с операцией безналичной оплаты товаров и услуг с использованием Карты требуется ввод ПИН-кода.

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), в том числе:

- путем рассылки электронных писем и сообщений от имени банков, популярных брендов, различных сервисов (Rambler, Mail.ru) или внутри социальных сетей с требованием ввести либо подтвердить свои персональные данные под различными предлогами;
- с помощью специальных вредоносных программ (вирусов), которые позволяют получить доступ ко всей информации, вводимой в компьютер.

С целью снижения таких рисков запрещается:

- следовать по ссылкам, указанным в подобных электронных письмах и сообщениях (включая ссылки на Сайт Банка), так как 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 операции 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, размещенные на Сайте Банка.

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

- либо использовать Карту с отдельным Карточным счетом, открытую только для совершения операций 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 операций 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 операций 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 операции, так как похожие адреса (добавлены дополнительные буквы и символы в адрес Интернет сайта) могут использоваться для осуществления неправомерных действий.

4.7. Перед совершением операции 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 подтверждённый 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. Не следует следовать по ссылкам, указанным в сообщениях (sms-сообщениях, электронных сообщениях, письмах и пр.), полученных от незнакомых лиц, для совершения операции оплаты на сайтах объявлений, в социальных сетях и иных сайтах сети Интернет.

4.9. 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 Интернет-магазинов, своей почты и других систем.

4.10. В целях повышения безопасности проводимых в сети Интернет операций с использованием реквизитов карт платежной системы «Мир», Банком применяется технология Mir Accept (3D-Secure). Использование данной технологии позволяет Банку осуществлять дополнительную идентификацию Клиента посредством проверки вводимого Клиентом одноразового пароля, поступающего в виде sms-сообщения на зарегистрированный в Банке Номер мобильного телефона Клиента / Push-уведомления, при совершении операции. Банки, обслуживающие Интернет-магазины и поддерживающие технологию Mir Accept (3D-Secure), как правило, размещают на своем сайте логотип MirAccept. Если технология 3D-Secure не поддерживается банком, обслуживающим Интернет-магазин, операция проводится в обычном режиме без ввода дополнительного пароля.

4.11. При совершении операции через Интернет Клиент обязан внимательно читать сообщение с одноразовым паролем, направленное Банком. Перед вводом одноразового пароля Клиент обязан убедиться, что сумма и наименование магазина в sms-сообщении совпадают с суммой операции и названием магазина, где Клиент совершает операцию.

4.12. При совершении операций через Интернет не следует отказываться от чека. Магазин обязан выдать чек Клиенту. Электронный чек приравнивается к бумажному, имеет юридическую силу и является полноценным документом, подтверждающим совершение операции.

5. Получение ПИН-кода с использованием Системы IVR

5.1 При обращении Клиента/Держателя (звонок рекомендуется осуществлять на третий рабочий день после получения новой Карты, обязательно с Номера мобильного телефона, который был указан Клиентом в Заявлении) в Единую службу поддержки клиентов проводится его идентификация по следующим данным:

- последние 4 цифры Карты и ФИО Держателя;
- номер мобильного телефона, указанный в Заявлении;
- кодовое слово;
- данные документа, удостоверяющего личность Клиента/Держателя.

5.2 После идентификации осуществляется перевод в Систему IVR, в которой посредством голосовых информационных сообщений предоставляется ПИН-код.

5.3 В случае если при вводе запрашиваемых Системой IVR данных Клиентом/Держателем была допущена ошибка, Система IVR предлагает ввести данные еще раз (не более двух повторных запросов).

5.4 После получения ПИН-кода Клиенту/Держателю необходимо активировать Карту и полученный ПИН-код, совершив операцию в банкомате Банка / стороннего банка (например, запрос баланса по Карте), за исключением Неэмбоссированной Карты (в том числе Карты СОГАЗ) / Карты-браслета, активацию которой осуществляет Банк после выдачи Держателю.

5.5 В течение срока действия Карты Клиенту/Держателю предоставляется возможность повторно получить ПИН-код к действующей Карте с использованием Системы IVR (Карта должна быть активна, то есть не заблокирована, ее действие не приостановлено). Взимание комиссионного вознаграждения за оказание данной услуги устанавливается Тарифами.

6. Правила безопасности при использовании Mir Pay, Токена

6.1. Держатель обязан соблюдать следующие правила по безопасности и конфиденциальности при работе с Mir Pay/Токеном:

- исключить передачу третьим лицам Мобильного устройства, в памяти которого хранятся данные Токена, а также пароля доступа к Mir Pay;
- в случае утраты Мобильных устройств, в памяти которых сохранены данные Токенов, а также в случаях Компрометации Токена незамедлительно информировать Банк по телефонам круглосуточной Единой службы поддержки клиентов с целью блокировки Токена и предотвращения несанкционированного проведения операций;
- для входа в Mir Pay не использовать внешние ссылки с других ресурсов, вход осуществляется только через иконку Mir Pay, установленного на Мобильном устройстве;
- не сообщать третьим лицам, даже сотрудникам Банка, свои пароли, коды проверки подлинности Карты (код CVC2/CVV2/ППК2), Кодовые слова, а также Одноразовые коды, поступающие на Мобильное устройство;
- избегать на своем Мобильном устройстве настроек типа «root» и «jailbreak» или иного взлома операционной системы;
- использовать только официальные версии Mir Pay, размещенные в Репозитории Google Play;
- устанавливать на Мобильное устройство и использовать актуальную версию Mir Pay;

- обеспечивать соответствующий уровень безопасности на Мобильном устройстве, используя антивирусное программное обеспечение (при наличии для данного типа Мобильного устройства), а также регулярно проводить его обновление;
- при смене Номера мобильного телефона обратиться в Банк;
- не переходить по ссылкам, направляемым на Мобильное устройство, на котором установлено Mir Pay;
- проверять реквизиты операций в sms-сообщениях/Push-уведомлениях от Банка;
- не оставлять Мобильное устройство без присмотра;
- обеспечить соответствующий уровень безопасности на Мобильном устройстве, используя средства аутентификации, встроенные в Мобильное устройство и предлагаемые провайдером сотовой связи;
- проводить проверку Мобильного устройства на предмет отсутствия регистрации средств аутентификации третьих лиц;
- не разглашать третьим лицам собственные средства аутентификации на Мобильном устройстве, являющиеся конфиденциальной информацией;
- удалить все личные данные, финансовую информацию и Токены с Мобильного устройства, использование которого прекращено, или при необходимости передачи устройства в организацию, осуществляющую ремонт;
- обратиться в круглосуточную Единую службу поддержки клиентов незамедлительно, в случае подозрений на любое несанкционированное использование Мобильного устройства или размещенного в платежном приложении Токена, а также в случае утраты Мобильного устройства;
- не блокировать любые функции безопасности, предусмотренные на Мобильных устройствах в целях защиты Токена;
- использовать Mir Pay, подключаясь только к проверенным источникам сети Интернет, не использовать Mir Pay при подключении к беспроводным сетям общего доступа.

6.2. Соблюдать правила безопасности при безналичной оплате товаров и услуг с использованием Токена, установленные в п. 3 настоящих Правил.