РЕАЛИСТ БАНК

Памятка
держателя платежной карты

Акционерное общество «Реалист Банк»

Тел. +7 (499) 968-94-23 Факс +7 (499) 968-94-23 E:mail:mailbox@realistbank.ru
http://www.realistbank.ru

1. Общие условия пользования

Карта является собственностью АО «РЕАЛИСТ БАНК» и предоставляется Вам во временное пользование. Карта действительна до последнего дня месяца года, указанного на лицевой стороне карты. Если Вы за 30 (тридцать) календарных дней письменно не уведомите Банк о своем намерении прекратить использование карты, она будет перевыпущена Банком на новый срок.

При использовании карты денежные средства Держателя карты списываются со счета его карты в пределах остатка средств на нем. За совершенные с использованием карты операции взимается плата в соответствии с Тарифами Банка.

Карта не подлежит передаче другому лицу. Пользование картой третьим лицом рассматривается Платежной Системой VISA International как грубое нарушение Правил использования платежной карты и влечет за собой прекращение обслуживания Клиента по инициативе Банка.

Карта предоставляется в неактивном состоянии. Для того, чтобы активировать карту, необходимо совершить операцию с использованием ПИН-кода.

2. Оплата товаров и услуг

С помощью карты Вы можете расплачиваться за товары и услуги практически во всех странах мира. О такой возможности Вы можете узнать по фирменной эмблеме VISA, которая обязательно размещается торгово-сервисным предприятием (далее – ТСП), принимающим к оплате карты, на видном для посетителей месте: на входных дверях, витринах, на кассовых аппаратах и т.д. Независимо от того, ведется ли Ваш счет в рублях РФ или долларах США, Вы можете осуществить платеж за товары и услуги в любой стране мира, где принимаются платежные карты VISA, в местной валюте.

Чтобы расплатиться за товары или услуги, Вам необходимо передать карту кассиру или иному работнику ТСП. По правилам приема к оплате платежных карт, на некоторых предприятиях у Вас могут попросить предъявить паспорт или иной документ, удостоверяющий личность.

При оплате с помощью карты товаров и услуг работником предприятия оформляется чек терминала или платежная квитанция (слип), если операция осуществляется с помощью импринтера. Убедившись в подлинности карты, работник предприятия производит авторизацию (получение разрешения на осуществление операции). Если операция разрешена, работник предприятия предлагает Вам подписать чек терминала (2 копии) или слип (3 копии). Ввод ПИН-кода при операции считается цифровым аналогом собственноручной подписи. При подписании документа необходимо проверить правильность заполнения суммы операции и других реквизитов. Не забудьте оставить себе один экземпляр чека или слипа! Работник предприятия обязан сличить Вашу подпись, поставленную в его присутствии на чеке терминала или слипе, с образцом подписи на карте. Ваша подпись на чеке (слипе) должна совпадать с образцом Вашей подписи на карте. Если работник учреждения не уверен в идентичности Вашей подписи, он имеет право отказать в оплате Вашей покупки по карте и предложить Вам иной способ оплаты, например, наличными.

При совершении операции оплаты в иностранном ТСП Вы заключаете договор с ТСП на поставку товара, оказание услуг или совершение инвестиционных операций. При этом следует иметь в виду, что заключение договора может осуществляться посредством совершения действий по выполнению условий, указанных в оферте. Совершение данных действий будет считаться принятием предложения заключить договор на условиях оферты. Вам необходимо внимательно ознакомиться с условиями договора с ТСП до момента оплаты товаров (услуг), заранее оценив риски утраты денежных средств. Защита гражданами

Российской Федерации своих прав в случае недобросовестности иностранных ТСП может быть затруднительной вследствие необходимости применения норм иностранного законодательства. Вам необходимо осуществлять взаимодействие с ТСП в соответствии с договором, в том числе в случаях, когда ТСП не была оказана либо некачественно оказана оплаченная с использованием платежной карты услуга, не была осуществлена поставка оплаченного товара.

Бесконтактная оплата картой Вы можете воспользоваться бесконтактной оплатой при наличии знака бесконтактной оплаты на лицевой стороне карты и в точках, обозначенных логотипами платежных систем с бесконтактными технологиями. Бесконтактные операции совершаются в режиме «самообслуживания» — Вы не передаете карту кассиру, а самостоятельно прикладываете ее к считывающему устройству терминала для проведения операции. Подсказки о порядке совершения операции выводятся на экран терминала (ПИН-клавиатуры). Операции, совершаемые бесконтактным способом, могут проводиться без ввода ПИН-кода или подписи Клиента на чеке в случаях, когда сумма операции не превышает лимит, установленный Банком для торгово-сервисного предприятия. Совершение операций на сумму свыше установленного лимита подтверждается вводом ПИН-кода либо подписью на чеке терминала. Кассир торгово-сервисного предприятия может попросить Вас предъявить карту для сверки подписей на карте и на чеке, при этом постарайтесь скрыть платежную информацию карты (номер карты, срок действия и CVV-код).

Операции в Интернет. Избегайте осуществления Интернет-операций с использованием карты в местах, где услуги Интернет являются общедоступными, например, в Интернет-кафе. Старайтесь пользоваться проверенными интернет-магазинами, в надежности, которых вы уверены. При оплате покупок в сети Интернет Вас попросят ввести код безопасности CVC2/CVV2 (трехзначный код, нанесенный в правой части полосы для подписи справа от последних четырех цифр номера карты). Этот код вводится для повышения безопасности Интернет-операций с использованием карт. Не сообщайте реквизиты Вашей банковской карты (номер карты, срок действия, трехзначный код безопасности, нанесенный на полосе для подписи, ПИН-код).

3. Получение наличных денежных средств

Используя карту, Вы можете получить наличные средства двумя способами.

В пунктах выдачи наличных в офисах Банка. Процесс получения наличных средств проходит в том же порядке, что и в случае оплаты товаров и услуг с помощью карты, при этом у Вас попросят предъявить паспорт или иной заменяющий его документ.

В банкоматах. При получении денег в банкомате Вы должны вставить карту в приемное устройство банкомата таким образом, чтобы магнитная полоса была обращена вниз и оказалась справа. После этого на экране появится надпись: "НАБЕРИТЕ СВОЙ ПИН-код", затем Вы должны выполнить все команды банкомата, отраженные на его экране. После предложения "ВОЗЬМИТЕ ВАШУ КАРТУ" необходимо без промедления взять карту, иначе по истечении 45 секунд она возвратится в банкомат. Предложенные банкоматом наличные следует также забирать без промедления. После получения наличных необходимо дождаться квитанции о проведенной операции.

В банкомате Вы можете узнать остаток на своем карточном счете.

Следует помнить, что в банкоматах, как правило, устанавливается дневной или единовременный лимит снятия наличных, в случае превышения которого Вы получите отказ. При необходимости снятия большой суммы наличности лучше обратиться со своей картой и паспортом в пункт выдачи наличных. С полным списком банкоматов и пунктов выдачи наличных Банка Вы можете ознакомиться на сайте Банка: **https://www.realistbank.ru**

4. Пополнение счета карты

Пополнение счета карты может осуществляться путем внесения наличных денежных средств в пунктах выдачи наличных РЕАЛИСТ БАНКа или безналичным путем.

При этом необходимо иметь в виду, что:

- все средства, перечисленные безналичным способом на карточный счет, становятся доступными на карте не позднее банковского дня, следующего за днем их зачисления на карточный счет;
- средства, внесенные в пунктах выдачи наличных, становятся доступными на счете платежной карты в режиме реального времени.
- Средства перечисленные с другой карты становятся доступными на карте не позднее 3 рабочего дня с момента перевода.

Реквизиты для безналичного перечисления рублевых средств на счет карты указаны в п.7 настоящей Памятки.

5. Меры безопасности

При получении карты Вам также выдается ПИН-код, который неизвестен никому, кроме Держателя карты, в том числе, никому из сотрудников Банка. ПИН-код может выдаваться либо с специальном запечатанном конверте, либо по телефону с помощью автоматического голосового робота, либо в сообщении SMS на Ваш телефон с соблюдением всех мер информационной защиты, предусмотренными международными нормами для такого вида сообщений. Банк самостоятельно определяет средство выдачи Вам ПИН-кода.

Персональный идентификационный номер (далее – ПИН-код) является одним из основных средств защиты карты от несанкционированного использования при снятии наличных денег в банкомате. Клиент несет ответственность за все операции, совершенные с использованием ПИН-кода, поэтому необходимо сохранять его в тайне.

Помните, что карта и ПИН-код являются ключами доступа к Вашему счету. Во избежание пользования деньгами на Вашем счете посторонними лицами необходимо: поставить свою подпись на оборотной стороне карты; запомнить или где-либо записать ПИН-код.

- Конверт или SMS-сообщение со значением ПИН-кода желательно уничтожить.
- запись ПИН-кода хранить отдельно от карты;
- не использовать карту в организациях торговли и обслуживания, не вызывающих доверия;
- при совершении операций с картой без использования банкоматов не выпускать ее из поля зрения;
- не пользоваться устройствами, которые требуют ввода ПИН-кода для доступа в помещение, где расположен банкомат;
- не использовать ПИН-код при заказе товаров либо услуг по телефону/факсу или по сети Интернет;
- при наборе кода в банкомате заслонять клавиатуру от посторонних глаз;
- не оставлять карту в местах, где кто-либо мог бы скопировать номер карты и Вашу подпись.

Обязательно сохраняйте все экземпляры документов (копии чеков и слипов), подтверждающих совершение операций по карте, по меньшей мере, в течение 120 календарных дней.

Соблюдайте общие правила хранения карты: не подвергайте карту воздействию источников теплового и электромагнитного излучения (динамики, магнитные застежки на сумочках и портмоне, ручные металлодетекторы), не допускайте механического воздействия на карту (царапины, искривления).

Осторожно, мошенники! (некоторые способы, используемые карточными мошенниками)
Банкомат

Для того, чтобы узнать ПИН-код, мошенники могут наклеивать на клавиатуру банкомата специальную прозрачную пленку с микросхемой, которая фиксирует вводимый ПИН-код или устанавливать жесткую накладку, полностью имитирующую клавиатуру банкомата. Специальное приспособление крепится также и на приемное устройство для карты для считывания информации с магнитной полосы. Затем, сняв «жучки», мошенники получают всю необходимую информацию о карте. Поэтому, при пользовании банкоматом не ленитесь внимательно осмотреть его и убедиться в отсутствии каких-либо «накладок» и посторонних устройств. Если вы заметили что-либо подозрительное, откажитесь от использования данного банкомата. Часто мошенники подсматривают ПИН-код в момент снятия денежных средств в банкомате держателем карты. Затем, карта похищается у держателя и с нее, в течение 10-15 минут, снимается вся оставшаяся на карте сумма. Пожалуйста, примите все меры, чтобы вводимый Вами ПИН-код был не заметен для окружающих. Известны случаи, когда мошенники в момент выдачи денежных средств отвлекают держателя карты, тем самым давая возможность другому мошеннику, стоящему рядом, забрать денежные средства, выданные банкоматом. Не отвлекайтесь, пока не получите деньги и карту из банкомата.

Интернет

Один из способов получения реквизитов карт, используемых мошенниками, заключается в создании «поддельного» интернет-магазина. Небольшой, недавно открытый магазин предлагает приобрести по картам товары и услуги. При этом, как в настоящем магазине, требуется ввести сведения о карте, только сведения эти передаются не в информационный центр платежной системы, а прямиком в базу данных мошенников. Чтобы избежать подобного обмана старайтесь пользоваться проверенными интернет-магазинами, в надежности, которых Вы уверены. Как правило, надежный интернет-магазин предлагает проведение платежа с использованием сертифицированных средств защиты информации: протокола SSL (Secure Socket Layer) или стандарта SET (Secure Electronic Transaction). Эта информация отражается в правом нижнем углу экрана. В российском сегменте сети Интернет зафиксированы случаи появления Web-сайтов, на которых предлагаются различные финансовые услуги с использованием банковских карт международных платежных систем. Пользователям предлагается заполнить электронные формы и указать реквизиты банковских карт, включая ПИН-код. При этом передача конфиденциальной информации ведется без использования защищенных протоколов информационного обмена. Этот и ряд других признаков, характеризующих работу подобных Web-сайтов, дает основания полагать, что такими предложениями могут маскироваться мошеннические действия, известные как «фишинг», т.е. заманивание пользователей с целью раскрытия конфиденциальной информации посредством использования поддельных Web-сайтов.

Обращения к держателям карт от имени Банка (фишинг)

Один из способов получения данных о карте и ее держателе состоит в том, что мошенники обращаются к держателю по телефону с сообщением от имени Банка или платежной системы, касающимся безопасности его карточного счета или проверки правильности данных. Например, что с картой производятся мошеннические действия и для их предотвращения держателю необходимо как можно быстрее перезвонить по определенному номеру телефона. При звонке по этому номеру держателя просят сообщить или ввести с клавиатуры телефона данные карты и свои персональные данные. В таких мошеннических обращениях, которые часто производятся с помощью автоответчика, отсутствует упоминание имени и фамилии держателя. Поэтому, пожалуйста, обращайте внимание на то, чтобы обращение к Вам было по фамилии, имени, отчеству. Если этого не происходит — налицо признаки мошенничества. Важно не перезванивать по номерам телефонов, указанных в подобных сообщениях. Звонить можно только по номеру, указанному на оборотной стороне карты. О подозрительных обращениях к Вам от имени Банка или платежной системы немедленно сообщайте в Банк посредством

дистанционного обслуживания. Другой способ, который используют мошенники для получения конфиденциальной информации от держателя карты, заключается в направлении держателю сообщения по электронной почте от имени Банка или платежной системы с уведомлением о подозрениях на компрометацию данных его карты, в котором держателя просят подтвердить эти данные, зайдя по определенной ссылке на сайт платежной системы (на самом деле, ссылка переадресует на сайт, созданный мошенниками). Если к Вам поступило подобное сообщение, ни в коем не сообщайте данных своей карты и немедленно обратитесь в Банк посредством дистанционного обслуживания. 10 из 10 Для незаконной активации карт мошенники звонят клиенту от имени Банка и под предлогом уточнения персональных данных получают у клиента всю информацию, указанную в Заявлении-Анкете. Помните, что Банк направляет Вам SMS-сообщения о выпуске и активации карты. При получении SMS-сообщений о действиях, которых Вы не совершали, немедленно обратитесь в Банк. Актуальные номера телефонов размещены на сайте Банка по адресу: realistbank.ru . Если при звонке от имени Банка у Вас возникли сомнения в принадлежности номера Банку, Вы можете позвонить по номерам, указанным на сайте или обратиться в Банк по каналам дистанционного обслуживания. При любых подозрительных обращениях к Вам от имени Банка немедленно проинформируйте об этом Банк .

6. Что делать при утрате карты

В случае утраты карты немедленно свяжитесь со службой поддержки Банка или процессингового центра КартСтандарт по круглосуточным телефонам: 8-800-770-79-20, 8-495-924-75-00, 8-383-363-11-58.

7. Реквизиты для перечисления денежных средств на счет карты

Реквизиты АО «РЕАЛИСТ БАНК»	
Полное наименование	Акционерное общество «Реалист Банк»
Сокращенное наименование	АО «РЕАЛИСТ БАНК»
Адрес	Российская Федерация, 109004, г. Москва, ул. Станиславского, дом 4, строение 1
ИНН	3801002781
КПП	770901001
ОКПО	09125424
Платежные реквизиты	
к/с 30101810245250000285 в ГУ Банка России по ФО БИК 044525285	
Реквизиты Держателя карты	
Номер Счета карты	
Ф.И.О. Держателя карты (полностью)	

При возникновении любых других вопросов по операциям с картой, Вы можете обращаться по телефонам: 8-499-968-94-23, 8-800-770-79-20.