

к Условиям обслуживания физических лиц при предоставлении и использовании банковских карт ПС «Мир» АКБ «НООСФЕРА» (АО) к Приказу №61/1 от 10.04.2017г.

ПАМЯТКА ДЕРЖАТЕЛЯМ БАНКОВСКИХ КАРТ АКБ «НООСФЕРА» (АО) ПО СОБЛЮДЕНИЮ МЕР БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ БАНКОВСКИХ КАРТ

1. ОБЩИЕ МЕРЫ БЕЗОПАСНОСТИ И МИНИМИЗАЦИИ РИСКОВ

Карта является собственностью АКБ «НООСФЕРА» (АО) (далее Банк) и предоставляется клиенту во временное пользование. Срок действия Карты указан на лицевой стороне Карты, после его истечения Карту рекомендуется сдать в Банк. При желании клиент может получить Карту на новый срок действия.

При получении Карты необходимо проставить на ней свою подпись.

Карта предназначена для проведения операций в торговых и сервисных точках, в банковских учреждениях и банкоматах, на которых размещены эмблемы соответствующих платежных систем.

ПИН-код (персональный идентификационный номер) — это комбинация цифр, содержащая 4 знака, предназначенная для идентификации Держателя Карты и защиты от несанкционированного ее использования. Информация о ПИН–коде должна быть известна только владельцу Карты. Никто не вправе требовать информацию о ПИН–коде Карты.

Запрещается хранить ПИН-код и Карту вместе, записывать ПИН-код на самой Карте.

ПИН-код необходимо хранить отдельно от Карты в недоступном для посторонних месте.

Не рекомендуется передавать Карту посторонним лицам (в том числе родственникам) для проведения каких-либо операций, за исключением сотрудников Банка и торгово-сервисных организаций.

Не рекомендуется передавать информацию по Вашей Карте посторонним лицам (номер Карты, ПИН-код, срок окончания действия Карты, ПКК2 — код безопасности) — данная информация может быть использована злоумышленниками в мошеннических целях.

Необходимо внимательно относиться к условиям хранения и использования банковской Карты.

Не подвергайте банковскую Карту механическим, температурным и электромагнитным воздействиям, а также избегайте попадания на нее влаги. Банковскую Карту нельзя хранить рядом с мобильным телефоном, бытовой и офисной техникой.

Рекомендуется в течение 6 месяцев со дня совершения операции по Карте сохранять чеки и слипы с оттиском Карты, подтверждающие оплату товаров и услуг. Если сделка по каким-либо причинам не состоялась, сохраняйте чеки о неуспешных операциях с использованием Карты. Указанные документы могут потребоваться для подтверждения правомерности операции, совершенной с использованием Карты, или для урегулирования спорных ситуаций.

Рекомендуется регулярно (не реже одного раза в месяц) проверять выписки по банковскому счету. При возникновении вопросов, связанных с проведенными операциями по счету (несанкционированными списаниями или ошибочными начислениями), необходимо незамедлительно обратиться в Банк.

В целях контроля над операциями с использованием Карты Банк предлагает услугу "SMS-сервис", с помощью которой можно получать информацию о доступном остатке по Карте, уведомлении о поступлении денежных средств на карточный счет и расходных операциях по счету. Услуга "SMS-сервис" предоставляется в соответствии с тарифами Банка по пластиковым картам, информацию о которых можно получить на сайте Банка: www.noosferabank.ru в разделе «Банковские карты».

При возникших подозрениях о несанкционированном использовании Вашей Карты (Карта была утеряна, украдена, захвачена банкоматом) для ее срочной блокировки необходимо немедленно обратиться в Банк по телефонам: Службы клиентской поддержки: 8-(495) 924-75-00; 8-(383) 363-11-58; (круглосуточно), либо отдел банковских карт и технологий Банка по телефону +7 (388-22) 241-11, (время работы: с 9ч.00мин. до 18ч.00мин. местного времени).

Не позднее пяти рабочих дней после блокировки Карты необходимо подать заявление в Банк, в котором должны быть указаны причина блокировки Карты и намерение Клиента на дальнейший перевыпуск Карты.

Информацию (номера телефонов) Службы поддержки клиентов Банка рекомендуется всегда иметь при себе, но отдельно от Карты.

Для информационного взаимодействия с Банком рекомендуется использовать реквизиты средств связи (мобильных и стационарных телефонов, факсов, интерактивных web-сайтов/порталов, обычной и электронной почты и пр.), которые указаны в документах, полученных в Банке.

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) – они могут вести на сайты-двойники.

Рекомендуется установка на персональный компьютер антивирусного программного обеспечения, регулярное его обновление, а также обновление других используемых Вами программных продуктов (операционной системы и прикладных программ) – это может защитить Вас от проникновения вредоносных программ.

2. МЕРЫ ПРЕДОСТОРОЖНОСТИ ПРИ СОВЕРШЕНИИ ОПЕРАЦИЙ С ИСПОЛЬЗОВАНИЕМ БАНКОВСКОЙ КАРТЫ В ТОРГОВО-СЕРВИСНЫХ ОРГАНИЗАЦИЯХ И БАНКОМАТАХ

Все операции с Картой в торгово-сервисных организациях необходимо совершать только при личном присутствии. Нельзя разрешать сотрудникам торгово-сервисной организации уносить Карту в другое помещение. Не допускайте потери Карты из поля Вашего зрения при проведении операций — информация с Вашей Карты при помощи специальной аппаратуры может быть скопирована для изготовления поддельной Карты с целью получения доступа к Вашему банковскому счету.

Перед тем как поставить подпись на слипе с оттиском Карты или чеке, необходимо убедиться, что в документе правильно указаны все данные о совершаемой операции. Если обнаружены неточности в указанной информации, следует отказаться от проставления подписи и попросить отмену проведенной операции. В случае отмены операции необходимо получить чек об отмене операции.

При возврате покупки или отказе от услуг, ранее полученных в торгово-сервисной точке по Вашей Карте, должна быть проведена операция «возврат покупки» с обязательным оформлением чека (слипа), на котором указан «возврат покупки», подписанного кассиром торгово-сервисной точки. Необходимо сохранить чек (слип) операции «возврат покупки». Если сумма операции не поступит на Ваш счет в течение 30 дней, рекомендуется обратиться в Банк для оформления заявления о спорной транзакции.

Не оставляйте в торгово-сервисных организациях незаполненные слипы с оттиском Вашей Карты (т.е. слипы, на которых отсутствует Ваша подпись и/или сумма операции). Незаполненные, а также «испорченные» слипы с оттиском Карты должны уничтожаться сотрудником торгово-сервисной организации сразу же в Вашем присутствии.

Не выбрасывайте и не оставляйте в торгово-сервисных организациях платежные документы по операциям с Картой – на них может быть отпечатан полный номер Карты.

Перед набором ПИН-кода во время совершения операции в торгово-сервисной организации следует убедиться в том, что люди, находящиеся в непосредственной близости, не смогут его увидеть. При вводе ПИН-кода необходимо обращать внимание на то, чтобы он вводился на специальном устройстве (ПИН-паде), непосредственно соединенным с кассовым аппаратом или платежным терминалом. Нельзя поддаваться на предложение ввести ПИН-код дважды на различных устройствах. Сотрудник банка или торгово-сервисной организации при проведении операции по Карте вправе потребовать документ, удостоверяющий Вашу личность.

По требованию сотрудника Банка или торгово-сервисной организации, в которых осуществляется оплата товаров/услуг с помощью Карты, Карта может быть изъята. В данном случае необходимо потребовать Акт об изъятии Карты и незамедлительно связаться с Банком.

Не забывайте забрать Карту после совершения операции, убедившись при этом, что возвращенная Карта принадлежит Вам.

Предъявляйте Карту к оплате только в тех торгово-сервисных организациях, которые вызывают доверие.

Для минимизации рисков компрометации Карты рекомендуется отказываться от получения наличных денежных средств в торгово-сервисных организациях, занимающихся обналичиванием денежных средств. Для данных целей необходимо использовать пункты выдачи наличных или банкоматы, находящиеся в безопасных местах (подразделения банка, государственные учреждения, крупные торговые комплексы, гостиницы, аэропорты и т.п.).

Перед началом проведения операции в банкомате необходимо осмотреть его лицевую часть – поверхность над клавиатурой и устройство для приема Карты в банкомат, на которых не должны находиться прикрепленные посторонние предметы. В противном случае следует воздержаться от использования данного банкомата и по возможности уведомить организацию, установившую банкомат/терминал самообслуживания, об обнаруженных подозрительных устройствах.

В случае некорректной работы банкомата (долгое время находится в режиме ожидания, самопроизвольная перезагрузка), следует отказаться от его использования, отменить текущую операцию, нажав кнопку "Отмена", и дождаться возврата банковской Карты.

При приеме и возврате Карты банкоматом нельзя толкать или выдергивать Карту до окончания ее прерывистого движения в картоприемнике.

Неравномерное движение Карты не является сбоем и настроено для защиты Карты и денежных средств на банковском счете клиента.

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

Не допускайте ошибок при вводе ПИН-кода Карты. После 3-х неудачных попыток ввода ПИН-кода Карта будет заблокирована.

Не рекомендуется совершать операции на банкоматах, вблизи которых присутствуют подозрительные лица. Операции на банкоматах рекомендуется проводить в хорошо освещенных и безопасных местах, либо в пунктах выдачи наличных денежных средств.

Считыватель банковских Карт для обеспечения доступа в специальные закрытые помещения, где устанавливаются банкоматы и другие терминалы самообслуживания, не должен требовать ввода ПИН-кода! Если при входе в помещение установлено устройство, требующее ввод ПИН-кода, не пользуйтесь им.

При проведении операции с вводом ПИН–кода необходимо проследить, чтобы он не был виден окружающим. Для исключения возможности видеозаписи Ваших действий и просмотра информации о ПИН-коде рекомендуем прикрывать клавиатуру рукой. Не прибегайте к помощи посторонних лиц при проведении операций по Картам.

По завершении операции не забудьте получить деньги, Карту и квитанцию (чек) банкомата. В противном случае денежные средства и Карта по истечении 20-40 секунд будут задержаны банкоматом.

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

В случае захвата Карты банкоматом/устройством самообслуживания вследствие технических проблем, незамедлительно свяжитесь с организацией, обслуживающей банкомат/устройство самообслуживания для уточнения информации, когда и где можно будет получить Карту. Рекомендуется обратиться в Банк для временной приостановки действия Карты.

В случае неполучения в банкомате всей или части запрошенной суммы, а также возникновении проблем при совершении операции пополнения счета (на устройствах с функцией приема наличных денежных средств) необходимо обратиться в Банк для оформления заявления о возникшей проблеме.

3. МЕРЫ БЕЗОПАСНОСТИ ПРИ СОВЕРШЕНИИ ОПЕРАЦИЙ БЕЗНАЛИЧНОЙ ОПЛАТЫ ТОВАРОВ (РАБОТ, УСЛУГ) ПОСРЕДСТВОМ СЕТИ ИНТЕРНЕТ

(заказ по факсу/телефону)

С целью повышения безопасности и минимизации угрозы мошеннических действий, рекомендуется для оплаты покупок в сети Интернет использовать отдельную банковскую Карту, предназначенную только для указанной цели. Пополнение Карты на необходимую сумму рекомендуется проводить незадолго до совершения операций оплаты.

Во избежание компрометации банковской Карты и ПИН-кода рекомендуется, ни при каких обстоятельствах не вводить ПИН-код Карты при совершении операций безналичной оплаты товаров (работ, услуг) посредством сети Интернет или при заказе покупки по факсу/телефону.

При проведении операций безналичной оплаты товаров/услуг посредством сети Интернет Вас могут попросить указать ПКК2 (три цифры кода безопасности). Данное значение находится на оборотной стороне Карты (три последних цифры, напечатанные на полосе для подписи или справа от нее в специальном поле).

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.

При проведении операций в Интернет-магазинах необходимо убедиться в наличии опубликованных обязательств по защите данных клиента и присутствии на сайте контактных данных организации.

Рекомендуется совершать покупки только со своего компьютера в целях сохранения конфиденциальности персональных данных и/или информации о банковской Карте. В случае совершения покупки с использованием чужого компьютера не рекомендуется сохранять на нем персональные данные и другую информацию — после завершения всех операций убедитесь, что персональные данные и другая информация не сохранились.

3.1. Особенности проведения операции оплаты товаров (услуг) с использованием реквизитов Карты в Интернет-магазинах, поддерживающих программы «Мир» Ассерt

3D Secure — современная технология обеспечения безопасности интернет-платежей для Держателей Карт национальной платежной систему «Мир», которая позволяет проводить дополнительную аутентификацию Держателя при проведении им платежей в Интернет-магазинах, поддерживающих данную технологию, путем набора одноразового защитного кода.

Введенный Держателем защитный код не доступен продавцам Интернет-магазинов, операторам связи и другим предприятиям торговли (далее – предприятие торговли).

Для оплаты товаров (услуг) на сайте предприятия торговли Держателю необходимо указать следующие данные: номер Карты, срок ее действия, фамилию и имя Держателя Карты в латинской транслитерации (как указано на Карте), код безопасности (ПКК2).

Далее, сайт предприятия торговли показывает страницу Банка (эмитента Карты), на которой предлагается ввести дополнительный одноразовый защитный код. Одновременно Банк направляет на номер мобильного телефона SMS-сообщение, содержащее этот защитный код.

Держатель подтверждает операцию оплаты товаров (услуг) посредством специализированного интерфейса.

Правильно введенный защитный код подтвердит, что Держатель идентифицирован Банком, и оплата товаров (услуг) будет подтверждена.

Если одноразовый защитный код окажется неверным, оплатить товар (услугу) картой будет невозможно.

Если Держатель произвел действия, в результате которых уклонился от введения защитного кода, то Держатель отвечает за любые убытки, расходы, которые могут возникнуть у Держателя или Банка в результате неиспользования защитного кода.

Предприятия торговли, которые принимают платежи с использованием 3D Secure, можно узнать по



В случае, если предприятие торговли не использует технологию 3D Secure, надежность совершения оплаты товара (услуги) будет обеспечена в обычном режиме.