# ***Уважаемые клиенты - владельцы банковских карт.***

Не секрет, что были, есть и будут люди, желающие всегда обогатиться за счет других - *МОШЕННИКИ.*

В связи с этим просим Вас обратить внимание на меры предосторожности, которые необходимо соблюдать, чтобы не стать жертвой мошенников и избежать возможных негативных последствий, связанных с использованием банковских карт:

## *SMS-информирование (обязательная услуга при выпуске пластиковой карты)*

SMS-информирование несет справочный характер о всех операциях совершенных при помощи карты и/или ее реквизитов, но далеко не последнюю роль играет в предотвращении хищений денежных средств с карт клиентов, из-за неправомерных действий третьих лиц. Банк информирует клиента об изменении состояния его остатка/операциях, совершенных по карте и/или при помощи ее реквизитов путем направления SMS-сообщения **со специального номера 8000** на мобильный телефон владельца карты, указанного при регистрации. ***(Все SMS-сообщения, полученные с иных телефонов являются мошенническими).***

*Для получения текущего баланса по карте на мобильный телефон, необходимо сформировать и отправить SMS с текстом:* ***1 XXXX*** *(где XXXX – последние четыре цифры номера карты) на специальный номер* ***8000*** *с мобильного телефона, указанного при регистрации.*

***ВНИМАНИЕ!***

***Напоминаем, о необходимости своевременно уведомлять Банк об изменении номера телефона, который был предоставлен для подключения SMS-информирования. Во избежание отсутствия контроля с вашей стороны, действий проведения неправомерных операций с картой и/или с ее реквизитами.***

## *Рекомендации при совершении операций с банковской картой в банкомате*

1. Осуществляйте операции с использованием банкоматов, установленных в безопасных местах (например, в государственных учреждениях, подразделениях банков, крупных торговых комплексах, гостиницах, аэропортах и т.п.).
2. Не используйте устройства, которые требуют ввода ПИН-кода для доступа в помещение, где расположен банкомат.
3. В случае если поблизости от банкомата находятся посторонние лица, следует выбрать более подходящее время для использования банкомата или воспользоваться другим банкоматом.
4. Перед использованием банкомата осмотрите его на наличие дополнительных устройств, не соответствующих его конструкции и расположенных в месте набора ПИН и в месте (прорезь), предназначенном для приема карт (например, наличие неровно установленной клавиатуры набора ПИН). В указанном случае воздержитесь от использования такого банкомата.
5. В случае если клавиатура или место для приема карт банкомата оборудованы дополнительными устройствами, не соответствующими его конструкции, воздержитесь от использования банковской карты в данном банкомате и сообщите о своих подозрениях сотрудникам кредитной организации по телефону, указанному на банкомате.
6. Не применяйте физическую силу, чтобы вставить банковскую карту в банкомат. Если банковская карта не вставляется, воздержитесь от использования такого банкомата.
7. Набирайте ПИН-код таким образом, чтобы люди, находящиеся в непосредственной близости, не смогли его увидеть. При наборе ПИН-кода прикрывайте клавиатуру рукой.
8. 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 банковской карты.
9. После получения наличных денежных средств в банкомате следует пересчитать банкноты полистно, убедиться в том, что банковская карта была возвращена банкоматом, дождаться выдачи квитанции при ее запросе, затем положить их в сумку (кошелек, карман) и только после этого отходить от банкомата.
10. Следует сохранять распечатанные банкоматом квитанции для последующей сверки указанных в них сумм с выпиской по банковскому счету.
11. Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций с банковской картой в банкоматах.
12. Если при проведении операций с банковской картой в банкомате банкомат не возвращает банковскую карту, следует позвонить в кредитную организацию по телефону, указанному на банкомате, и объяснить обстоятельства произошедшего, а также следует обратиться в кредитную организацию — эмитент

банковской карты (кредитную организацию, выдавшую банковскую карту), и далее следовать инструкциям сотрудника кредитной организации.

***ВНИМАНИЕ!***

***Обращайте внимание на наличие посторонних (накладных) устройств на клавиатуре и картридере банкомата.***

***По возможности, не пользуйтесь банкоматом, вызывающим сомнение!***

***Старайтесь пользоваться банкоматами, установленные на территории ОАО «НК Банк», либо в других вызывающих доверие местах (государственные учреждения, крупные торговые центры, аэропорты, гостиницы и т.п.)***




### *Рекомендации при использовании банковской карты для безналичной оплаты товаров и услуг*

1. Не используйте банковские карты в организациях торговли и услуг, не вызывающих доверия.
2. Требуйте проведения операций с банковской картой только в Вашем присутствии. Это необходимо в целях снижения риска неправомерного получения Ваших персональных данных, указанных на банковской карте.
3. При использовании банковской карты для оплаты товаров и услуг кассир может потребовать от владельца банковской карты предоставить паспорт, подписать чек или ввести ПИН. Перед набором ПИН следует убедиться в том, что люди, находящиеся в непосредственной близости, не смогут его увидеть. Перед тем как подписать чек, в обязательном порядке проверьте сумму, указанную на чеке.
4. В случае если при попытке оплаты банковской картой имела место “неуспешная” операция, следует сохранить один экземпляр выданного терминалом чека для последующей проверки на отсутствие указанной операции в выписке по банковскому счету.

### *Рекомендации при совершении операций с банковской картой через сеть Интернет*

1. Не используйте ПИН при заказе товаров и услуг через сеть Интернет, а также по телефону/факсу.
2. Не сообщайте персональные данные или информацию о банковской(ом) карте (счете) через сеть Интернет (номер карты, срок действия банковской карты, пароли доступа к карте: ПИН-код, CVC/CVV).
3. Следует пользоваться интернет-сайтами только известных и проверенных организаций торговли и услуг. При расчетах в сети Интернет самостоятельно оценивайте надежность Торговой точки, Банк не гарантирует удовлетворение претензий в случае проведения интернет-операций через сомнительные Интернет-магазины.
4. 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.

5. Будьте внимательны, операции совершенные через интернет-сайты при помощи карты и/или ее реквизитов (а в частности ввода CVC/CVV-кода, что является аналогом ввода ПИН-кода) не оспариваются.

В связи с этим, убедительно напоминаем, что карта и/или ее реквизиты не должны предоставляться третьим лицам.

6. Рекомендуется совершать покупки только со своего компьютера в целях сохранения конфиденциальности персональных данных и(или) информации о банковской(ом) карте (счете).

В случае если покупка совершается с использованием чужого компьютера, не рекомендуется сохранять на нем персональные данные и другую информацию, а после завершения всех операций нужно убедиться, что персональные данные и другая информация не сохранились (вновь загрузив в браузере web-страницу продавца, на которой совершались покупки).

7. Установите на свой компьютер антивирусное программное обеспечение и регулярно производите его обновление и обновление других используемых Вами программных продуктов (операционной системы и прикладных программ), это может защитить Вас от проникновения вредоносного программного обеспечения.

8. Дополнительная услуга безопасности при использование пластиковых карт - электронных средств платежа (ЭСП) на интернет-сайтах - **3-D Secure**. Внешним признаком Интернет-магазина, подключенного к системе безопасности Международные платежные системы (МПС), является присутствие на веб-сайте уведомления для покупателей о том, что при оплате товаров и услуг с помощью карт используется технология 3-D Secure Verified by Visa и MasterCard SecureCode. Сайты, не подключенные к программе безопасности МПС должны вызывать недоверие - стоит отказаться от использования данных сайтов.

*Для подключения данной услуги вы можете воспользоваться Банкоматами ОАО «НК Банк» или ОАО «Банк Москвы». (Плата за предоставление данной услуги, взымается согласно действующим Тарифам ОАО «НК Банк»).*

***ВНИМАНИЕ!***

***Никогда не вводите ПИН-коды для своих банковских карт при любых операциях в сети Интернет. Для проведения интернет-транзакции ПИН-код не требуется. Пользуйтесь только теми web-сайтами, которым Вы доверяете!***

***Никогда не отвечайте на сообщения, полученные по электронной почте или SMS, в которых под какими-либо предлогами (блокировка карты, обновление программного обеспечения или сверка баз данных и т.п.) предлагается отправить по SMS или ввести с клавиатуры компьютера ваши персональные данные (ФИО, номера банковских карт, ПИН-коды CVC/CVV коды и т.п.).***

***В случае утраты (утери, хищения) карты, во избежание возможности ее использования третьими лицами, Держатель обязан незамедлительно известить об этом факте Банк по телефону, указанному на обратной стороне карты 8(495) 411-88-44, ежедневно (кроме субботы и воскресенья, праздничных и нерабочих по законодательству РФ дней) с 9,00 часов до 18,00 часов по московскому времени, либо по телефону 8(495) 728-77-88 круглосуточной службы поддержки ОАО «НК Банк» - Процессинговый Центр ОАО «Банк Москвы». При получении такого извещения и индификации клиента будет осуществлена блокировка карты.***

## Безопасные покупки в Интернете (технология 3-D Secure)

Дополнительная услуга безопасности при использование пластиковых карт - электронных средств платежа (ЭСП) на интернет-сайтах - **3-D Secure**. Внешним признаком Интернет-магазина, подключенного к системе безопасности Международные платежные системы (МПС), является присутствие на веб-сайте уведомления для покупателей о том, что при оплате товаров и услуг с помощью карт используется технология **3-D Secure Verified by Visa и MasterCard SecureCode.** Сайты, не подключенные к программе безопасности МПС должны вызывать недоверие (если только вы сами уверенны и доверяете данному сайту), и стоит отказаться от использования данных сайтов.

**Для подключения данной услуги вы можете воспользоваться**

**Банкоматом ОАО «НК Банк»,**

*Составлено по рекомендации ЦБ РФ (письмо 120-Т от 02.10.2009г.)*

**расположенного на 2-м этаже Банка**

**по адресу: 125047, г. Москва, Миусская площадь, д. 2:**

**Услуга предоставляется платно - 12$ в год за одну карту.**

**Как подключить и пользоваться услугой:**

1. Меню Банкомата «Услуги»/«Получить пароль для оплаты в интернете» далее заводите свой мобильный номер телефона).
2. Получите SMS-сообщение, что Ваша карта подключена к технологии безопасных интернет-платежей.
3. При совершении операции на защищенных интернет-сайтах на ваш мобильный телефон будет поступать SMS-сообщение с буквенно-цифровым кодом, который необходимо ввести для подтверждения покупки.

***С Уважением,***

***Управление пластиковых карт и платежных систем***

***ОАО «НК Банк»***