

Руководство по использованию услуги «Мобильный банк»

Передача SMS-сообщений может происходить по факту совершения операции по карте/счету или по запросу Клиента:

1. SMS-сообщения отправляются Клиенту при совершении следующих операций:

По банковской карте	По счету без карты
• выдача наличных денежных средств; • безналичная операция (оплата товаров/услуг, интернет-платежи); • запрос баланса в устройстве (банкомат, ПВН); • зачисление/списание денежных средств на/с карту(-ы); • отмена выдачи наличных денежных средств/безналичной операции; • возврат средств по безналичной операции; • внесение наличных денежных средств в cash-in; • активизация/блокировка карты; • смена ПИН-кода; • подключение/отключение услуг сервиса; • неуспешные операции по карте.	• поступление денежных на счет (при сумме поступления от 100 рублей) • списание денежных средств со счета (при сумме списания от 100 рублей)

Пример сообщения об операции оплаты товара по карте, выпущенной к рублевому счету:

Karta 0058: 28.10.2015 15:06, spisanie 538 RUR, ORENBURG 12 PUSHKINA\PRODUKTY. Dostupno 15620 RUR.

* Последние 4 цифры номера карты, позволяющие идентифицировать карту.

Типичные проблемы неполучения информационных SMS-сообщений и их устранение:

1. В заявлении неверно указан номер мобильного телефона. Необходимо обратиться в Банк и уточнить эту информацию.
2. Не хватает места для входящих SMS-сообщений в мобильном телефоне. Необходимо освободить место согласно инструкции мобильного телефона.
3. Мобильный телефон отключен или находится вне зоны действия сети. Сообщение хранится в SMS-центре, как правило, в течение 3-х дней с момента его формирования и отправки Банком и может быть доставлено в этот срок при включении Вашего мобильного телефона, или вхождения в зону действия сети.
4. В настройках Вашего лицевого счета мобильного телефона поставлен запрет получения сообщений с коротких номеров. Необходимо обратиться к оператору для отмены запрета.

Рекомендуемые меры безопасности

Для безопасного использования услуги «Мобильный банк» ПАО «НИКО-БАНК» рекомендует:

- установить на устройство мобильной связи антивирусное программное обеспечение с регулярно обновляемыми базами;
 - не переходить по ссылкам, приходящим из недостоверных источников, в том числе на известные сайты;
 - не скачивать на устройство мобильной связи приложения из непроверенных источников;
 - своевременно уведомлять Банк о смене номера телефона мобильной связи, который клиент предоставил Банку для получения услуги "Мобильный банк", в том числе, на который происходит информирование об операциях по счету клиента;
 - не передавать устройство мобильной связи для использования третьим лицам, в том числе родственникам;
 - в случае утраты устройства мобильной связи незамедлительно заблокировать sim-карту, сообщить об этом в Банк для блокировки услуги.