СБЕРБАНК
Всегда рядом

117997, Москва, ул. Вавилова, д. 19
Телефон: +7 (495) 500-55-50, 8 (800) 555-55-50
Факс: +7 (495) 957-57-31, +7 (495) 747-37-31
sberbank@sberbank.ru, www.sberbank.ru

дата _____

Долгая
Ксения Александровна

7905xxx1506
ksyushadolgaya@mail.ru

Исх. № 160610-0155-324300
от 28.06.2016

Уважаемая Ксения Александровна!

ПАО Сбербанк уведомляет, что Ваше заявление о следующей спорной операции рассмотрено:

№ п/п	Номер карты	Дата проведения	Дата обработки	Место совершения операции	Сумма / валюта
1.	427616XXXXXX4095	04.06.2016	04.06.2016	PEREVOD 676196XXXXXXXX0368	8000.00 RUR / 80.00 RUR (комиссия)

При рассмотрении обращения установлено, что услуга Мобильный банк подключена **25.04.2016** в устройстве самообслуживания по карте № 427616XXXXXX4095 к телефону **+ 7**905xxx1506 *(указан Вами как контактный)*. Операция подключения услуги совершена с использованием карты и подтверждена вводом ПИН-кода, который является аналогом подписи Держателя карты.

В Банк через услугу «Мобильный банк» поступил SMS-запрос о перечислении средств в общей сумме 8080.00 RUR со счета карты № 427616XXXXXX4095 для перевода на карту № 676196XXXXXXXX0368.

Банк выполнил обязательства по переводу средств получателя платежей.

07.06.2016 действие услуги прекращено.

В соответствии с Договором:

Предоставление услуг «Мобильного банка» осуществляется на основании полученного Банком Распоряжения в виде СМС-сообщения, направленного с использованием средства мобильной связи с номера телефона, указанного Держателем при подключении услуги «Мобильный банк» (далее - Сообщение).

Держатель подтверждает, что полученное Банком Сообщение рассматривается Банком как распоряжение (поручение) на проведение операций по счетам карт Держателя и на предоставление других услуг Банка, полученное непосредственно от Держателя.

В соответствии со ст. 854 ГК РФ списание средств со счета получателя платежа осуществляется только на основании распоряжения клиента (получателя платежей). Таким образом, Банк не имеет права на списание денежных средств со счета получателей.

В связи с этим, у Банка отсутствуют основания для возврата на счет карты оспариваемых Вами сумм.

Обращаем внимание, что указанный случай мог возникнуть вследствие несанкционированного доступа к Вашему мобильному телефону. Несанкционированный доступ возможен как физически (путем доступа к мобильному телефону неуполномоченных лиц), так и дистанционно (по причине вирусного заражения телефона. Подобные вирусы на телефонах обладают функционалом, который позволяет скрывать от владельца телефона SMS-сообщения от определенных номеров телефонов, перехватывать и отправлять с данного устройства любые SMS-запросы без ведома клиента).

Требования по информационной безопасности изложены в приложении к Договору банковского обслуживания и находятся в общем доступе на сайте Банка. Указанные в Договоре положения соответствуют требованиям Банка России.

В целях предотвращения возможных угроз Банк рекомендует:

1. Установить новое мобильное приложение Сбербанк Онлайн для смартфонов на платформе Android со встроенным антивирусом. Антивирус защищает не только операции и информацию в мобильном приложении, но и устройство в целом. После установки приложения, клиент может быть полностью уверен в сохранности средств. Антивирус продолжает проверять телефон на наличие вирусов, даже если клиент не пользуется приложением в данный момент. Официальное приложение Банка можно скачать только в магазине Google Play.
2. Следовать рекомендациям, которые помогают избегать киберугрозы, в том числе связанные с заражением вредоносным ПО. Подробнее с рекомендациями вы всегда можете ознакомиться на сайте Банка в разделе Меры Безопасности http://www.sberbank.ru/ru/person/dist_services/warning/.
3. Существует возможность управления быстрыми сервисами, которые позволяют мгновенно оплачивать мобильный телефон и переводить деньги с карты на карту с помощью SMS запроса. При необходимости можно отключить быстрые сервисы, направив SMS сообщение с текстом «0» (ноль) на номер 900.

Если Вы не направляли SMS-запрос, то вероятно имели место мошеннические действия третьих лиц посредством дистанционного доступа к Вашему мобильному устройству. Вам необходимо подать заявление на имя руководителя территориального подразделения «К» МВД России по области/субъекту. Данный вопрос находится в компетенции правоохранительных органов.

Ксения Александровна, надеемся, что вышеизложенные сведения помогли Вам разобраться в сложившейся ситуации и при соблюдении элементарных правил информационной безопасности позволят предотвратить повторение инцидента в будущем.

Всегда рады ответить на Ваши вопросы.

Старший специалист
Центр заботы о клиентах
ПАО Сбербанк **Романова К.Ю.**