

- оформить виртуальную карту с установлением размера индивидуального лимита, ограничивающего операции, в том числе с использованием других банковских карт;
- внимательно читать тексты СМС-сообщений и иных уведомлений с кодами подтверждений, проверять реквизиты операций. Если реквизиты не совпадают, то такой пароль вводить нельзя.

Когда банк считает совершаемые от имени клиента операции подозрительными, он может по своей инициативе временно заблокировать доступ к сервисам СМС-банка и онлайн-кабинета. Если операции совершены держателем карты, для быстрого возобновления доступа к денежным средствам достаточно позвонить в контактный центр банка.

В случае утери или смены номера телефона, привязанного к банковской карте, необходимо:

- связаться с банком для отключения услуги СМС-уведомления;
- заблокировать сим-карту, обратившись к сотовому оператору.

При возникновении малейших подозрений насчет предпринимаемых попыток совершения мошеннических действий следует незамедлительно уведомлять об этом банк.

Соблюдение приведенных мер и рекомендаций позволит предотвратить случаи дистанционного хищения денежных средств.