**Мошенничество с использованием банковских карт**

Мошенничество с использованием [электронных средств платежа](consultantplus://offline/ref=210AA3DCA1C1E73792E0EF1180E27BB5352CA6F958A471D3FB5743894120D132508656F0AE3D89749E986AD76B6518C507D337CDE625FF62g7SAG) (средств и (или) способов, позволяющих переводить денежные средства в форме безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств) наказывается по ст. 159.3 УК РФ наказывается лишением свободы на срок до 3 лет, а если гражданину причинен значительны ущерб на сумму свыше 5 тысяч рублей, - до 5 лет лишения свободы.

Данный вид мошенничества активно развивается вместе с возможностями электронных платежных средств. Повсеместное использование банковских карт для расчетов, в том числе в сети «Интернет» привлекает разного рода мошенников, которые постоянно находят новые способы добычи информации о держателях карт для несанкционированного снятия денежных средств.

Мошенничество с банковскими картами подразумевает использование ее данных для проведения операций без ведома или согласия законного владельца с карт-счетом.

Во избежание хищения денежных средств рекомендуется использовать простые правила безопасности при обращении с банковскими картами.

1. **Не доверяйте звонкам из «банка»**. Сотрудники банка имеют право спросить кодовое слово только в том случае, если вы сами им позвонили, а не наоборот. Если сомневаетесь в том, что это действительно звонить банковский работник - положите трубку.

Позвоните по номеру, который указан на вашей карте, и поговорите с реальной службой поддержки банка.

**2. Не сообщайте данные банковских карт, CVV-код и одноразовые пароли, приходящие по СМС**.

3. **Установите лимит по снятию наличных**. Данные карты могут похитить и с помощью скиминга - специального устройства, которое считывает данные карты и подсматривает ПИН-код (с помощью накладки на клавиатуру или мини-камеры). Этот способ применяется все реже, но операции со снятием наличных все же лучше минимизировать. Если мошенник ввел правильные цифры ПИН-кода на клавиатуре, доказать, что деньги в банкомате снимали не вы, практически невозможно.

Если вам не нужны крупные суммы наличными каждый день, установите минимальный дневной лимит на снятие наличных - это крупная сумма, которой могут поживиться мошенники. Если большой объем наличных потребуется вам самому, увеличить дневной лимит можно либо в мобильном приложении, либо через кол-центр банка. А потом снова опустить до безопасного уровня.

4. **Держите крупные сбережения на резервном счете, который не привязан к карте**. Счетов в банке у вас может быть несколько, карта обычно привязана только к одному. Основные средства лучше держать на том счете, который не привязан к карте. Если не хватает, можно прямо перед покупкой в мобильном приложении сделать перевод между своими счетами.

Если в отношении Вас совершено преступление с использованием Вашей банковской карты, следует незамедлительно сообщить об этом в правоохранительные органы, а также в выпустивший карту банк, для ее блокировки.

В соответствии с ч. 15 ст. 9 Федерального закона «О национальной платежной системе» банк обязан вернуть клиенту деньги, в случае если их списали без ведома владельца карты. Операцию нужно оспорить не позднее следующего дня с момента получения от банка уведомления о списании средств. Однако на практике в большинстве случаев человек сам сообщает мошенникам ПИН-код или CVC/CVV (код из трех цифр с обратной стороны карты), в связи с чем считается, что он добровольно дал согласие на перевод денег и банк обоснованно отказывает в возмещении потерь.