**Что такое компрометация карты?**

Использование банковского «пластика» – повседневность. Удобно, быстро и выгодно из-за программ лояльности. Однако владение банковской картой накладывает на ее владельца и обязанности. Прежде всего – это соблюдение правил безопасности при использовании этого платежного инструмента. Перечень запретов знаком практически каждому: не передавать карту третьим лицам, не сообщать пароли и коды, не хранить пароли вместе с картой, не хранить/не оставлять карту в общедоступном месте, при оплате использовать только проверенные платежные платформы, а при утере карты сообщать об этом банк и осуществлять ее блокировку.

При нарушении правил – она считается скомпрометированной. Что такое компрометация, как избежать этих проблем в [интервью Banki.ru](https://www.banki.ru/news/daytheme/?id=10982693) рассказа эксперт Центра финансовой грамотности НИФИ Минфина России Ольга Дайнеко.

Под компрометацией подразумевается утечка ключевой информации по карте (или риск такой утечки). Данные карты, пин-коды/пароли (в том числе-от интернет-банка или приложения)-важные данные, при утечке которых, если карту не заблокировать, пользоваться ей нельзя, поскольку после компрометации это может нанести владельцу карточного счета материальный ущерб.

Несмотря на то, что базовые правила безопасного пользования банковской картой известны если не всем, то большинству, мы все порой нарушаем правила, даже не замечая этого. Например, даем свою карту своему ребенку, супругу/супруге или близкому родственнику, забываем ее в «безопасном» месте-на столе на работе и многое другое. Совершая такие безобидные отступления, карта уже попадает под риск компрометации. Не потому, что родственник похитит данные карты, а потому что как только банковская карта перестает находиться у ее держателя, у него прекращается возможность контролировать ее безопасное использование. А ответственность за сохранность банковских данных всегда на ее владельце.

Формально деньги находятся в банке, а карта- это ключ клиента для возможности распоряжения ими. Если деньги с карты похищены, банк может нести за это ответственность только при одновременном соблюдении двух условий:

-клиент в течение суток после списания средств сообщил об этом в банк, написал заявление на возврат перечисленных со счета средств и заблокировал карту;

-списание средств с карты произошло без участия и без ведома владельца счета и он не нарушал правила безопасного использования карты (не сообщал пароли и коды, не передавал данные карты третьим лицам).

Если сообщить об операции, которую не совершал-дело техники, то доказать, что списание средств произошло без ведома владельца проблематично. Нередко доказывать этот факт приходится в судебном порядке.

Гарантированный возврат от банка похищенных средств можно получить лишь если банк:

-не уведомил клиента о списании денег;

- не обеспечил безопасность переводов и счетов;

- знал, что данные/карта похищены, но все равно осуществил трансакцию;

- имелись признаки, что операции совершаются без ведома клиента (несколько списаний подряд, нетипичные для клиента операции, операции с устройства/ на счет лицу, включенному в базу данных Банка России о попытках и случаях осуществления перевода денежных средств без согласия клиента), но не приостановил их исполнение;

- допустил техническую/иную ошибку, которая привела к потере средств клиента.

Случается, что банки сами блокируют карту (накладывают временные ограничения на операции) по признакам компрометации. Антифрод-системы банков помогают предотвратить мошеннические операции, в том числе те, которые совершаются без ведома владельца счета. Как правило это происходит по следующим признакам:

- если за коротки промежуток времени (подряд) происходит большое количество быстрых переводов, иная нетипичная для клиента активность по счету;

- подозрительный получатель перевода (например, номер телефона получателя или устройство, с которого производится перевод в «черном списке»;

- производится оплата через небезопасный сайт или платежную платформу (когда протоколы домена не соответствуют защите и данные карты могут быть похищены).

Чтобы не огорчаться внезапным списаниям со своего карточного счета, нужно соблюдать базовые правила и проявлять аккуратность по использованию этого средства платежа:

1. Не передавать карту не только постороннему, но и родственнику (будь то расчет в кафе или оплата проезда в транспорте). Банковская карта должна быть как зубная щетка, потому что финансовая гигиена не менее важна, чем личная.
2. Никогда и ни под какие правдоподобные объяснения просящего не сообщать банковские смс/push-уведомления, пароли/коды, СVV/CVC третьим лицам, как и не совершать под чьим-то «руководством» действия в банковском приложении или личном кабинете клиента банка;
3. Не держать карту вместе с пин-кодом, написанным на листке бумаги (например, в одной сумке или кошельке), не хранить на телефоне фото всех данных карты;
4. Не вводить данные от личного кабинета, мобильного приложения или пин-код на клавиатуре банкомата в присутствии постороннего, а при вводе прикрывать клавиатуру рукой;
5. Не совершать платежи на подозрительных сайтах и незнакомых платежных платформах;
6. Не входить в онлайн-банк/банковское мобильное приложение при использовании общедоступного (открытого) Wi-Fi или с общедоступного устройства (компьютера, планшета);
7. Не забирать карту, «съеденную» банкоматом, если ее достали не в вашем отсутствии-лучше перевыпустить;
8. При утере или краже карты, а также при обнаружении операции, которую не совершали, нужно незамедлительно связаться с банком и заблокировать карту (через мобильное приложение, интернет-банк или позвонив на горячую линию). При подозрительном списании также нужно подать заявление не только о блокировке счёта, но и об отзыве перевода. Нелишним будет и обращение в полицию с заявлением о мошеннических действиях.