**Хищения, совершаемые с использованием современных информационно-коммуникационных технологий**

Развитие технологий в современном мире обуславливает их повсеместное проникновение во все сферы общественной жизни. Этим пользуются не только добросовестные пользователи информационных сетей, но и злоумышленники, преследующие различные противоправные цели – личное обогащение, дискредитацию граждан и государственных органов, распространение запрещенной информации.

В Российской Федерации отмечается ежегодный рост таких преступлений. Повсеместно регистрируются преступления, связанные с хищением денежных средств из банков и иных кредитных организаций, физических и юридических лиц, совершаемых с использованием современных информационно-коммуникационных технологий, ответственность за которые в зависимости от способа преступного посягательства предусмотрена ст.ст. 158, 159, 159.3, 159.6 УК РФ.

Федеральным законом от 23.04.2018 № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» введена ответственность виновных лиц по статье 158 УК РФ за кражу, совершенную с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного статьей 159.3 УК РФ).

Аналогичным образом, с целью усиления уголовной ответственности за противоправные действия с использованием электронных средств платежа, изменены диспозиции и санкции статей 159.3 и 159.6 УК РФ.

Среди наиболее распространенных способов хищений прокурорско-следственная практика выделяет:

- использование злоумышленниками индивидуальных данных банковских карт пострадавших для осуществления расчетов в преступных целях. Такие ситуации возможны при компрометации этих карт в результате раскрытия их данных третьим лицам;

- двойное списание, характеризующееся тем, что потерпевший передает банковскую карту продавцу (оператору, официанту, заправщику), которую тот дважды проводит через платежный терминал под предлогом ошибки при первоначальном платеже;

- хищение при бесконтактной оплате, в тех случаях, когда похитители оперируют собственными бесконтактными считывателями или терминалами, прислоняя их к карманам и сумкам;

- хищение с использованием дубликата сим-карты мобильного телефона, которое осуществляются путем предварительного выяснения преступниками номера сим-карты, к которому привязаны банковские карты и изготовления ее фальшивого аналога с последующим списанием денежных средств;

- хищения посредством использования информации о банковских картах, предоставленных похитителям самими пострадавшими для оплаты продаваемых ими товаров;

- распространенный характер носят хищения, связанные с обманом доверчивых граждан, когда похитители, представляясь сотрудниками службы безопасности банка, сообщают Вам, что «банк выявил подозрительную операцию» или «в системе произошел сбой», просит у вас полные данные карты, CVV- или CVC-код, код из СМС или пароли от Сбербанк Онлайн. Это нужно якобы «для сохранности ваших денег». Сразу заканчивайте разговор. Работник банка никогда не попросит у вас секретные данные от карты или интернет-банка.

Настоятельно просим не откликаться на такие провокации, сохранять бдительность и в каждом случае поступления сомнительных предложений от неизвестных лиц сообщать о них в компетентные органы для уголовно-правовой оценки и организации уголовного преследования злоумышленников.

Помощник прокурора

Юхновского района П.Д. Минченков