Межрайонной прокуратурой проанализировано состояние преступности по профилактике, пресечению, раскрытию и расследованию хищений, совершенных с использованием электронных средств платежа.

Указанный вид преступлений стал актуален в связи с развитием информационных технологий, что позволяет их совершать дистанционно, с минимальными рисками для преступников.

Федеральным законом от 23.04.2018 N 111-ФЗ "О внесении изменений в Уголовный кодекс Российской Федерации" усилена уголовная ответственность за хищение денежных средств с банковского счета или электронных денежных средств, в том числе с использованием электронных средств платежа.

Как следует из Пояснительной записки к законопроекту, изменения направлены на повышение уголовно-правовой защиты граждан и организаций путем усиления уголовной ответственности за хищение чужого имущества, совершенного с банковского счета, а равно электронных денежных средств, в том числе потому, что общественную опасность указанных деяний усиливает специфика способа совершения преступления - использование удаленного доступа к банковскому счету при помощи технических средств, позволяющего лицу оставаться анонимным и совершать преступление из любой точки мира, имея лишь доступ к сети Интернет, который может быть рассчитан на многократное применение, в том числе использоваться для доступа не только к банковским счетам, но и иным охраняемым и особо охраняемым данным.

При этом такие действия виновного могут найти разную уголовно-правовую квалификацию.

Так, в ч. 3 ст. 158 УК РФ введен п. "г" - кража, совершенная с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159.3 УК РФ).

Для квалификации по этому пункту необходимо, чтобы действия виновного были тайными, то есть в отсутствие собственника, иных лиц либо незаметно для них.

Наиболее распространенным видом преступлений в настоящее время являются именно кражи денежных средств со счетов граждан. При этом преступники, завладев путем обмана цифровыми кодами либо персональными данными карт, похищают денежные средства дистанционно.

Как тайное хищение следует квалифицировать действия и тогда, когда виновным потерпевший введен в заблуждение или обманут, под воздействием чего он сам передает злоумышленнику свою карту или сообщает персональный идентификационный номер - пин-код, а снятие денег с банкомата происходит без потерпевшего.

По указанному критерию по ст. 158 УК РФ надлежит квалифицировать и действия, связанные с перехватом информации с пластиковых карт с использованием, например "хакерских ридеров" - специальных устройств, способных перехватывать электронные сигналы, или специальных устройств, устанавливаемых в карточкоприемник банкомата.

Понятие электронного средства платежа дано в п. 19 ст. 3 Федерального

закона от 27.06.2011 N 161-ФЗ "О национальной платежной системе". Это средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств.

Хищение денежных средств с банковского счета, а равно в отношении электронных денежных средств возможно и путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, что является специальным видом мошенничества и влечет уголовную ответственность по п. "в" ч. 3 ст. 159.6 УК РФ.

Таким образом, неотъемлемым признаком объективной стороны такого преступления будет обязательное оказание незаконного воздействия на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети. В противном случае, учитывая тайный способ хищения, действия должны быть квалифицированы как кража, даже если снятие денежных средств совершено путем использования учетных данных собственника, полученных путем обмана последнего или использования его мобильного телефона, подключенного к услуге "мобильный банк".

Например, в производстве СО ОМВД России по району Кунцево г. Москвы находится уголовное дело, возбужденное следователем по признакам преступления предусмотренного ч. 2 ст. 159 УК РФ в отношении неустановленного лица.

Изучением материалов уголовного дела установлено, что не позднее 11.04.2018, неустановленное лицо, представившееся сотрудником службы безопасности ПАО «ВТБ», посредством телефонного звонка под предлогом проверки безопасности банковской карты, путем установления цифровых кодов, завладело денежными средствами в размере 185 000 рублей 00 копеек, принадлежащими ФИО.

В соответствии с п. 17 Постановления Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», в случаях, когда лицо похитило безналичные денежные средства, воспользовавшись необходимой для получения доступа к ним конфиденциальной информацией держателя платежной карты (например, персональными данными владельца, данными платежной карты, контрольной информацией, паролями), переданной злоумышленнику самим держателем платежной карты под воздействием обмана или злоупотребления доверием, действия виновного квалифицируются как кража.

Таким образом, действия неустановленного лица квалифицированы как кража с банковского счета, а равно в отношении электронных денежных средств.

Единственным надежным способом защиты от такого рода преступлений является бдительность граждан, которым нельзя передавать персональные данные

и индивидуальные коды банковских карт третьим лицам, в том числе представляющимся в ходе телефонных разговоров сотрудниками служб безопасности банков.

Следует учесть, что при обнаружении подозрительных операций, кредитная организация самостоятельно блокирует расчетные счета, и никакие подтверждающие коды для этого не требуются.

Манипуляции с банковскими картами можно проводить только в отделениях банков, либо через официальные мобильные приложения.