

МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ БАНКОВСКИХ КАРТ

Никитина Ксения Сергеевна

магистрант Федерального государственного автономного образовательного учреждения высшего образования Санкт-Петербургский государственный университет аэрокосмического приборостроения, РФ, г. Санкт-Петербург

За период с 2018 года по настоящее время банковские карты стали неотъемлемой частью жизни современного общества. Тем не менее, всеми удобствами и преимуществами использования платежных карт начинают пользоваться и мошенники в своих корыстных целях. Каждый год правоохранительными органами выявляются новые методы, к которым прибегали преступники, совершая тот или иной вид мошенничества с помощью банковских карт.

Постановление Пленума Верховного Суда РФ 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» гласит, если в случае хищения денег виновно лицо использует злоупотребление доверием или обман, данные действия должны быть квалифицированы по статье 159.3 УК РФ (ред. от 23.04.2018 № 111-ФЗ) «Мошенничество с использованием платежных карт».

Согласно Уголовному кодексу Российской Федерации, если ущерб, который был нанесен держателю карты незначителен, а именно, он составляет 2500 рублей, то преступление относится к административному. В том случае, если материалы дела дошли до правоохранительных органов, то данное преступление может быть квалифицировано не только по ст. 159.3 «Мошенничество с использованием платежных карт». Противоправные действия, совершенные в данной сфере, зачастую квалифицируются по нескольким статьям Уголовного кодекса, как: ст.158 «Кража», ст. 159.1 «Мошенничество в сфере кредитования», ст. 159.6 «Мошенничество в сфере компьютерной информации», ст. 187 «Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов», ст. 273 «Создание, использование и распространение вредоносных компьютерных программ».

Мошенничество, связанное с банковскими картами кроме непосредственного объекта – денег, в большинстве случаев затрагивает отношения, которые складываются в сфере безналичных расчетов, также, как и использование компьютерных технологий, для поиска и добычи конфиденциальной информации. Данное обстоятельство провоцирует многочисленные ошибки квалификации, которые встречаются в правоприменительной деятельности.

Кроме хорошо изученных приемов мошенничества с банковскими картами, таких как призывы помощи через смс-сообщения, отправление вирусов на технические устройства с помощью рассылки через электронную почту вирусосодержащие объекты и создание поддельных банкоматов, грабители все чаще начинают использовать новые методы: скимминг и фишинг, так как видят в этих способах хорошие условия, для получения выгоды.

Скимминг – форма преступления, при которой происходит кража личностных данных с платежной карты посредством специального считывающего устройства (скиммера). Лица, совершающие преступление, создают копию, которая содержит всю информацию, собранную с магнитной полосы платежной карты. Также злоумышленники узнают ПИН-код с помощью накладок на клавиатуре или камеры, которую устанавливают в помещение, где стоят банкоматы.

Фишинг— вид интернет-мошенничества, при которой преступники стараются выманить

конфиденциальные данные граждан. Данный вид преступления производится путём проведения массовых рассылок писем от имени различных торговых сетей или брендов на электронную почту, а также через личные сообщения внутри различных сервисов и социальных сетей. Нередко в подобных письмах содержится гиперссылка на интернет ресурс, который внешне неотличимый от настоящего. Различными психологическими приемами злоумышленники стараются побудить пользователя ввести данные своей платежной карты на фальшивом веб-сайте. В том случае, если страница сайта была замаскирована под банк, то появится сообщение, которое будет гласить, о ложном техническом сбое в системе и потребует внести данные платежной карты, для ее восстановления. В случае использования фальшивого сайта под видом онлайн магазина потребуется ввести все сведения при оплате покупок. Вследствие данных действий мошенники получают доступ к банковским счетам.

Основной проблемой при расследовании мошенничества с банковскими картами является низкая оперативность следственных действий, а также запутанность схем вывода денежных средств с банковских счетов мошенников. Первым пунктом стоит отметить тот факт, что номера подобных счетов, в большинстве случаев, не имеют регистрации в электронных системах хранения денежных средств, таких как КИВИ, Яндекс. Деньги и др. Правонарушители используют сим-карты, также не прошедшие регистрацию паспортных данных в салонах мобильной связи. Второй проблемой, требующей рассмотрения, является большой путь денежных средств, которые совершаются при переводе от первого подставного счета до счета, которым владеет непосредственно мошенник. Отслеживание транзакции - процесс, требующий больших временных затрат. В том случае, если сумма ущерба составляет сумму меньше 5000 рублей, правоохранительные органы не успевают вычислить мошенника, потому как успевают истечь сроки давности преступления. На данный момент категория мошенничеств с банковскими картами является самой не раскрываемой. Однако правоохранительными органами производится целый ряд мер, по борьбе с преступностью и такой специфической категории: - использование современных технологий по отслеживанию изготовления платежных карт; - поиск новых кадров, имеющих техническое образование, чей высокий профессионализм помогает в борьбе с мошенниками. К материальным следам преступления данного вида относится сама карта как подлинная, но не принадлежащая мошеннику, так и карта со следами подделки. В большинстве случаев при обыске у преступников обнаруживаются пластиковые карты белого цвета, на которые нанесена магнитная полоса, считывающие устройства для банкомата (скиммеры), микрокамеры, через которые фиксируются ПИН-код.

При определении подозреваемых, способных совершить подобное преступление рассматриваются лица, хорошо разбирающиеся в электронной технике, которые хорошо знакомы с процессами копирования информации с банковских карт и нанесения ее на пластиковую карту, также обладающие навыками программирования. Стоит отметить рост преступности в сфере банковской деятельности и использовании банковских карт за последние несколько лет, в связи с чем, необходимо поднимать уровень информационной безопасности в банковской сфере, а также в сфере по борьбе с экономическими преступлениями: направить значительные средства на образование сотрудников правоохранительных органов, увеличение штата сотрудников с целью повышения уровня раскрываемости данной категории преступлений, дабы идти не в ногу с преступностью, а идти на опережение.

Список литературы:

1. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 07.04.2020) [Электронный ресурс] URL: <http://www.consultant.ru/>
2. Козодаева О.Н., Обыденнова А.С. Способы совершения мошенничества с использованием банковских карт // Право – 2019.
3. Сазонов М.М. Виды мошенничеств с банковскими картами и совершенствование мер виктимологического предупреждения // Виктимология – 2018 - №2(16).

4. Стародубова И.С. Юридические и практические аспекты мошенничества в финансово-кредитной сфере // «Экономика и бизнес» - 2017.

5. Табак И.С. Мошенничество с банковскими картами // Современные инновации – 2018 - №4 (26).