УДК 343.9

ОСОБЕННОСТИ РАСКРЫТИЯ МОШЕННИЧЕСТВА, СОВЕРШЕННОГО С ИСПОЛЬЗОВАНИЕМ ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Екимцев Сергей Валерьевич. Старший преподаватель кафедры оперативно-разыскной деятельности ОВД.
Орловский юридический институт МВД России имени В.В. Лукьянова.
Служебный адрес: 302027, Российская Федерация, г. Орел, ул. Игнатова, д. 2.

В статье исследуется цифровое мошенничество, которое на сегодняшний день является глобальной проблемой для всех экономик мира. Основной причиной распространения данной проблемы можно считать бурное развитие компьютерных и интернет технологий. Раскрываются виды мошенничества, а также способы его совершения. Описаны схемы, которые часто применяются в мошенничестве. В заданном контексте приведены наиболее типичные следственные ситуации, складывающиеся на первоначальном этапе расследования мошенничества, совершенного с использованием информационно-коммуникационных технологий. Изложены особенности допроса лиц, проходящих по уголовным делам о хищениях, совершенных с использованием телекоммуникационных технологий, в качестве потерпевших.

Ключевые слова: цифровизация; мошенничество; хищения; информационно-коммуникационные технологии; допрос.

FEATURES OF DISCLOSURE OF FRAUD COMMITTED WITH THE USE OF TELECOMMUNICATION TECHNOLOGIES

Ekimtsev Sergey Valer'evich. Senior teacher of the chair of Operational-Investigative Activities of the Internal Affairs Bodies.
Lukyanov Orel Law Institute of the Ministry of the Interior of Russia.
Work address: 302027, Russian Federation, Orel, st. Ignatova 2.

The article explores digital fraud, which today is a global problem for all economies in the world. The main reason for the spread of this problem can be considered the rapid development of computer and Internet technologies. The types of fraud, as well as ways of committing it, are revealed. Schemes that are often used in fraud are described. In the given context, the most typical investigative situations that develop at the initial stage of the investigation of fraud committed using information and communication technologies are given. The features of the interrogation of persons involved in criminal cases of theft committed with the use of telecommunication technologies as victims are outlined.

Keywords: digitalization; fraud; embezzlement; information and communication technologies; interrogation.

Современное развитие экономики идет по пути цифровизации. Её всё чаще называют веб-экономика, интернет-экономика, электронная экономика, в некоторых источниках встречается такой термин как цифрономика. В связи с этим широкое распространение получило цифровое мошенничество в финансовой сфере.

К числу основных видов таких преступлений можно отнести [1, с. 720-727]:

а) мошенничества, совершенные путем создания фиктивных объявлений о продаже товаров, либо оказании услуг, при которых потерпевший перечисляет денежные средства преступнику самостоятельно одним из указанных мошенником способов;

б) мошенничества, связанные с реализацией товаров и услуг потерпевшим посредством сети Интернет, когда преступник связывается с продавцом или поставщиком услуг и в процессе общения убеждает последнего подключиться к его абонентскому номеру услуги мобильного или интернет-банкинга, после чего преступник получает доступ к банковским счетам потерпевшего и похищает денежные средства;

в) хищение денежных средств с банковских счетов граждан, доступ к управлению которыми преступник получает в результате заражения смартфона потерпевшего вирусной программой, позволяющей использовать услуги интернет-банкинга.

Безусловно, практике противодействия хищениям, совершенным дистанционным способом, характерно наличие ряда проблем организационно-тактического и правового характера. К числу наиболее острых проблем можно отнести недостаточный уровень подготовки оперативных сотрудников, способных противостоять преступлениям указанных видов. Данная проблема обусловлена отсутствием у них опыта раскрытия таких преступлений, а также недостаточным уровнем профессиональной подготовки. Об этом свидетельствует анализ образовательного процесса, который показывает, что даже в тематических планах дисциплин оперативно-розыскной специализации отсутствуют занятия, посвященные рассмотрению вопросов выявления, предупреждения, пресечения и раскрытия хищений денежных средств граждан, совершенных удаленным способом, что крайне негативно сказывается на процессе подготовки высококвалифицированных кадров [2, с. 127].

Существуют следующие мошеннические схемы [3, с. 52]:

1. Дамп и памп. Относительно простой вид аферы. Мошенники искусственно раздувают цены на непопулярные токены, распространяя неверную информацию и всячески их рекламируя.

2. Облачный майнинг заключается в проверке достоверности данных с опорой на общественное мнение. Чем достоверность выше, тем больше вероятность, что мошенники ещё не применили свои схемы. Также необходимо использовать только проверенные серверы для поиска информации. Есть несколько трюков, которые чаще всего используют мошенники: отсутствие информации о создателях сервиса, скрытый домен, регистрация компании в престижном городе, все директора – иностранные резиденты.

3. Многоуровневые маркетинговые схемы состоят из прямых продаж только в сфере криптовалют. Отлично оформленная визуализация заставляет клиента поверить, что деньги можно заработать легко и быстро. Идентифицировать схемы легко, так как у них есть общая черта: они фактически не продают товар или услуги, а вместо этого приглашают пользователей присоединиться к группе с большим количеством уровней и требуют внесения определённой платы для старта заработка. В итоге схема оказывается обычной финансовой пирамидой.

4. Инвестиционные схемы. Криптовалюта является непредсказуемой системой, которая обладает высокой волатильностью (изменчивостью цен). Следовательно, если поступают предложения о ежедневных доходах и участие в проекте с гарантированным возвратом средств – стоит усомниться в достоверности и не искушаться получением легких денег.

5. Поддельные ICO и криптовалюты. Группа китайских экспертов во время мониторинга рынка обнаружила более 4000 фейковых криптовалют и десятки фальшивых

ICO. Авторитетная компания и известные разработчики с меньшей вероятностью будут мошенниками, чем анонимные создатели, пусть даже с крутым сайтом и whitepaper.

Преступления данной категории отличаются от традиционных краж и мошенничеств тем, что приносят злоумышленникам большой доход при относительно небольших рисках. Это связано с рядом особенностей [4, с. 82]:

- скрытность совершаемых преступником действий: существует множество программных и технических средств, обеспечивающих анонимность пользователя;
- оперативность производимых действий: отправка сообщений потенциальной жертве и электронные платежи занимают секунды;
- интеллектуальный характер. Хищения в сети «Интернет» и использование вредоносного программного обеспечения преступной деятельности: злоумышленник зачастую владеет знаниями и навыками в области программирования на порядок выше потенциальной жертвы;
- дистанционный характер преступления: преступник и потерпевший могут находиться как в разных городах, так и в разных странах. Зачастую зрительный контакт отсутствует, о личности и внешнем облике злоумышленника ничего не известно;
- возможность автоматизированного совершения преступлений;
- много эпизодный характер преступных действий при множественности потерпевших;
- многообразие и постоянное обновление способов и форм совершения преступлений;
- латентность совершаемых преступлений: не все пострадавшие обращаются в правоохранительные органы, а в некоторых случаях даже и не знают о хищении у них денежных средств (например, когда с одного и того же счета происходит планомерное хищение небольших сумм).

Все эти факторы значительно затрудняют процесс раскрытия данной категории преступлений. Проведение технических мероприятий и сложных компьютерных экспертиз всегда занимает некоторое время, что, с учетом легкости изменения и уничтожения компьютерной информации, делает их не всегда эффективными.

Анализ уголовных дел о мошенничествах с использованием телекоммуникационных технологий, позволяет выделить наиболее типичные следственные ситуации. Они как элемент частных криминалистических методик расследования отдельных видов преступлений формируются не произвольно, а на основе эмпирического анализа совокупности репрезентативных эмпирических источников, что является неотъемлемым условием выявления именно устойчивых, существенных, отчетливо выраженных, систематически повторяющихся черт, присущих расследованию соответствующих деяний. Данная дифференциация следственных ситуаций важна не как самоцель, а как подход, позволяющий предложить правоприменителю более точные и адресные рекомендации по организации расследования, более рациональному и тактически верному воздействию на те условия, с которыми ему приходится иметь дело [5, с. 54-60].

С учетом этого наиболее типичными следственными ситуациями первоначального этапа являются:

1. Установлено хищение денежных средств, совершенное с использованием электронных средств платежа, единовременно или серийно, в отношении потерпевшего, утратившего контроль за принадлежащей ему банковской картой, реквизитами счета, контактным номером, иными средствами защиты банковского счета.

2. Установлено серийное хищение денежных средств, совершенное с использованием электронных средств платежа и применением методов социальной инженерии, компьютерных технологий, иных способов целенаправленного воздействия на потерпевшего и/или принадлежащие ему электронные устройства.

Следователи и орган дознания обязаны [6, с. 57]: произвести работу с потерпевшим, затем допросить его. Допрос лиц, проходящих по уголовным делам о преступлениях названной категории, осуществляется, в целом, в соответствии с рекомендациями, разработанными для этого следственного действия, с акцентированием внимания на всестороннем установлении обстоятельств, во-первых, образующих общий предмет доказывания согласно ст. 73 УПК РФ; во-вторых, определяющих специфику указанных деяний, проявляющихся в конструкции их состава.

С учетом проанализированных ранее факторов виктимности следователю необходимо строить тактику допроса потерпевших, выражая максимальную [7, с. 56-65] доброжелательность и вежливость к лицам, проявившим недостаточную правовую, финансовую или техническую компетентность, а равно подвергнувшимся психологическому воздействию злоумышленников. Тем более нередко потерпевшими от данных деяний, в особенности совершенных с помощью методов социальной инженерии (иными словами, совершенных лицами, специализирующимися на систематическом хищении денежных средств с помощью электронных средств платежа), выступают лица старших возрастных групп, которые в силу естественных психофизиологических процессов являются максимально уязвимыми.

Например, по уголовному делу о серийном совершении хищений денежных средств граждан с банковских карт с помощью использования сервиса ПАО «Сбербанк» «Мобильный банк», была допрошена группа потерпевших, содержание показаний которых было, в целом, аналогичным. Допрошенный проживает в определенном городе, имеет банковскую карту (дебетовую зарплатную, кредитную или иную карту) ПАО «Сбербанк»: VISA, МИР (и пр.), привязанную к счету № ХХХ, открытому в соответствующем отделении сбербанка. В определенную дату ему на мобильный телефон пришло смс-сообщение о начислении заработной платы/пенсии (либо об ином начислении денежных средств), спустя некоторое время, через банкомат (приложение «Сбербанк онлайн» и т.п.) обнаружил отсутствие на карте существенной денежной суммы. Обратившись на «горячую линию» Сбербанка, либо посетив офис и т.д., допрашиваемый узнал, что с его карты был осуществлен перевод другому (конкретному) человеку, к чему допрашиваемый отношения не имеет и с этим человеком незнаком. До списания денежных средств на телефон приходило сообщение об обновлении «флеш-плеера», что допрашиваемый и сделал, после чего телефон стал вести себя атипично: не включался, не заряжался и т.п. Пользовался сотовым телефоном с операционной системой «Андроид», к карте был привязан номер телефона № ХХХ, также подключена услуга «мобильный банк» с полным пакетом. При этом никаких смс-сообщений о подтверждении перевода и о переводе не приходило. Ущерб для потерпевшего является значительным.

По мере установления психологического контакта необходимо, побудив допрашиваемого к свободному рассказу, а также направляя его мысли путем постановки детализирующих и конкретизирующих вопросов, установить следующую совокупность обстоятельств:

1) обстоятельства, связанные с открытием банковского счета и оформлением в данной связи банковской карты (иного электронного средства платежа), а также с техническим обеспечением использования данного счета:

- дата, место, цель открытия банковского счета, наименование и подразделение банка, выдавшего карту, либо оформившего иное электронное средство платежа, условия и особенности банковского обслуживания;

- вид, номер, наименование банковского счета, а также соответствующего ему банковской карты (дебетовая, кредитная, карта рассрочки, накопительная, социальная);

внешняя форма карты: пластиковая или виртуальная и т.д., наименование электронного кошелька, иные реквизиты счета (карты);

- наименование оператора мобильной связи и номер мобильного телефона, привязанный к банковскому счету / банковской карте, электронному кошельку; на имя какого лица зарегистрирован данный контакт, в каких отношениях это лицо находится с потерпевшим;

- наименование, модель, марка и иные характеристики мобильного устройства (мобильного телефона, смартфона, планшетного устройства и т.д.), к которому подключена сим-карта, привязанная к банковскому счету; наименование и криминалистически значимые характеристики иного электронного устройства, на которое установлено программное обеспечение для совершения финансовых операций в дистанционном формате;

- программное обеспечение для совершения финансовых операций, установленное на мобильном телефоне и/или ином электронном устройстве, кем и когда оно установлено; наименование и технические особенности данного программного обеспечения, значимые с точки зрения способов совершения и сокрытия преступлений и т.п.;

2) обстоятельства, связанные с текущим использованием банковского счета и соответствующей ему банковской карты (пластиковой, виртуальной), электронного кошелька, предшествующие совершению деяния:

- каким образом, с какой периодичностью, с применением каких электронных средств платежа использовались счет и/или карта потерпевшим;

- круг лиц, имеющих доступ, а также право и/или возможность систематически совершать операции по данной карте; на каких условиях, в каких пределах и/или лимите;

- имели ли место обстоятельства, в результате которых иные лица (помимо тех, кому потерпевший лично доверял использование своей карты/счета) могли получить возможность узнать реквизиты счета/карты, носящие конфиденциальный характер и т.п.;

- сумма денежных средств, находившаяся на банковском счете потерпевшего, до момента незаконного доступа к банковскому счету и хищению, из каких источников она сформировалась (поступила);

3) обстоятельства, связанные с полной ли частичной утратой доступа к банковскому счету либо контроля за хранящимися на нем денежными средствами:

- где, когда, каким образом потерпевшему стало известно о неправомерном доступе иных лиц к его банковскому счету;

- действовали ли эти лица путем непосредственного вербального контакта либо с помощью средств связи; знакомы ли потерпевшему эти лица, если знакомы, то в каких отношениях находились;

- каково было последовательное содержание действий этих лиц и корреспондирующих им действий потерпевшего; какого характера персональную информацию субъекты преступления называли или сообщали в СМС, письме на электронную почту и т.д. (каким образом обращались к потерпевшему, какие данные относительно счета, карты, обслуживающего банка, а равно якобы попытки совершения несанкционированной финансовой операции иными лицами они указывали, какие меры предлагали осуществить потерпевшему);

- какими действиями и иными мерами потерпевший отреагировал (например, какие посетил сайты, скачал (из каких источников) или открыл электронные приложения, ссылки, мессенджеры и т.д.), какую именно персональную информацию и каким образом он сообщил злоумышленникам;

- что побудило допрашиваемого вступить с ними в вербальный контакт или электронную переписку, отнестись с доверием к сообщенной ими информации как к достоверной, выполнить определенные действия по их просьбе или требованию, а равно по собственной инициативе под воздействием навязанной ему легенды;

- каков итог взаимодействия потерпевшего с данными лицами;

- каковы приметы и иные характеризующие особенности этих лиц, а также использованные ими средства связи (контактные данные);

- каков вред причинен потерпевшему в результате совершения преступления, из каких слагаемых он состоит.

Отсюда, предмет допроса потерпевшего, при совершении мошенничества с использованием средств сотовой связи, может составить установление следующих основных обстоятельств:

- способ связи с потерпевшим: на сотовый или стационарный телефон поступил звонок (СМС, ММС);

- номер телефона, с которого поступил звонок (СМС, ММС);

- время поступления звонка потерпевшему;

- просьбы, предложения, которые были выдвинуты;

- кем представился преступник;

- о чем он говорил;

- какие действия предлагал выполнить и в связи с какими событиями,

- запомнил ли потерпевший голос преступника;

- может ли охарактеризовать его;

- сможет ли опознать преступника (по каким характерным признакам);

- какую сумму денежных средств и за какие услуги преступник просил передать;

- способ передачи денежных средств: если блиц-переводом – на чье имя (Ф.И.О.);

- адрес этого лица, если через посредника, то в какое время и в каком месте осуществлялась передача денег;

- подробное описание человека, которому были переданы деньги (может ли потерпевший его опознать и составить фоторобот);

- был ли посредник на автомобиле (описание транспортного средства, государственный номер автомобиля);

- если переводом на счет определенного номера сотового телефона - на какой номер сотового телефона была зачислена денежная сумма;

- иные обстоятельства, имеющие значение для уголовного дела: звонил ли потерпевший своим родственникам (например, при требовании денег за родственников по различным причинам);

- в какой момент, что было установлено из разговора;

- звонил ли потерпевший преступнику повторно, если да, то, о чем он говорил с ним, предлагал ли преступник передать ему еще денежные средства, если да, то за какие услуги, сделал ли это потерпевший, если нет, то почему.

Для получения доказательственной информации, на ряду с другими оперативно-розыскными мероприятиями и следственными действиями, важное значение имеет проведение такого оперативно-розыскного мероприятия как «получение компьютерной информации», представляющее собой негласное оперативно-розыскное мероприятие, осуществляемое с использованием возможностей оперативно-технических подразделений в целях копирования или изъятия сведений, содержащихся на жестком диске компьютера или на иных электронных носителях, связанных с компьютером каналом связи, если для их получения требуется получение к ним удаленного доступа по информа-

ционно-коммуникационным сетям, в том числе с применением заблаговременно внедренных закладных устройств и (или) программных компонентов [8, с. 30].

Исходя из вышеизложенного, можно сказать, что при раскрытии хищений денежных средств с использованием информационно-коммуникационным технологий очевидна необходимость в специальных знаниях.

ЛИТЕРАТУРА

1. Альгинова В.В. К вопросу о мошенничестве с использованием банковских карт // Аллея науки. 2018. Т. 2. № 11 (27). С. 720-727.

2. Завезёнова И.А., Краюшкин К.Д., Нестерова А.В., Ососко Я.С. Цифровое мошенничество в финансовой сфере: новые типы обмана в контексте дигитализации: материалы Международного студенческого научно-практического форума по финансовой грамотности Волгоградский государственный университет. 2018. С. 125-144.

3. Иногамова-Хегай Л.В. Квалификации преступлений с использованием компьютерных технологий // Уголовное право: стратегия развития в XXI веке: материалы XVI Международной научно-практической конференции. Москва: РГ-Пресс, 2019. С. 51-55.

4. Кузьмин И.А. Актуальные направления подготовки сотрудников ОВД, осуществляющих противодействие хищениям денежных средств с использованием информационно-коммуникационных технологий // Подготовка кадров для силовых структур: современные направления и образовательные технологии: материалы двадцать второй Всероссийской научно-методической конференции. Иркутск: ФГКОУ ВПО ВСИ МВД России, 2015. С. 81-83.

5. Князьков А.С. Следственная ситуация как предпосылка тактико-криминалистической деятельности следователя // Криминалистические чтения на Байкале-2012: материалы Всероссийской научно-практической конференции. Иркутск, 2012. С. 54-60.

6. Яковлев А.Н., Олиндер Н.В. Особенности расследования преступлений, совершенных с использованием электронных платежных средств и систем: научно-методическое пособие. М., 2012. 240 с.

7. Варданян А.В. Общие положения допроса свидетелей и потерпевших по делам о злоупотреблениях полномочиями лицами, выполняющими управленческие функции в коммерческих и иных организациях // Общество и право. 2017. № 3 (61). С. 130-134; Грибунов, О.П., Долматова М.О. Допрос как источник получения вербальной информации при расследовании хищений нефтепродуктов на объектах железнодорожного транспорта // Известия Тульского государственного университета. Экономические и юридические науки. 2020. № 1. С. 56-65.

8. Екимцев С.В. Особенности проведения оперативно-розыскного мероприятия «получение компьютерной информации» // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2019. № 2(79). С. 27-30.