Журнал правовых и экономических исследований.
Journal of Legal and Economic Studies, 2022, 2: 7–12

АКТУАЛЬНАЯ ТЕМА

DOI 10.26163/GIEF.2022.28.99.001
УДК 343.72:(005.932.5:004.087):343.98

A.V. Bachieva, T.O. Boziev

CRIMINAL AND CRIMINALISTIC CHARACTERISTICS OF E-PAYMENT FRAUD

Albina Bachieva – senior lecturer, the Department of Criminal Law, State Institute of Economics, Finance, Law and Technology, PhD in Law, associate professor, Gatchina; **e-mail: albinab07@mail.ru**.
Taulan Boziev – Head of the Department of Criminal Law, State Institute of Economics, Finance, Law and Technology, PhD in Law, associate professor, Gatchina; **e-mail: boziev1975@yandex.ru**.

We consider criminal and criminalistic characteristics when detecting and investigating e-payment fraud. Methods and forms of fraud using e-payments are analyzed. We describe circumstances to be stated and proved when committing the fraud in question.

Keywords: *fraud; online payments; internet technologies; electronic methods of payment; cybercrime.*

А.В. Бачиева, Т.О. Бозиев

УГОЛОВНО-ПРАВОВАЯ И КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКИ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА

Альбина Владимировна Бачиева – доцент кафедры уголовно-правовых дисциплин, Государственный институт экономики, финансов, права и технологий, кандидат юридических наук, доцент, г. Гатчина; **e-mail: albinab07@mail.ru**.
Таулан Османович Бозиев – зав. кафедрой уголовно-правовых дисциплин, Государственный институт экономики, финансов, права и технологий, кандидат юридических наук, доцент, г. Гатчина; **e-mail: boziev1975@yandex.ru**.

Статья посвящена исследованию уголовно-правовой и криминалистической характеристик при раскрытии и расследовании мошенничества, совершаемого с использованием электронных средств платежей. Проанализированы методы и формы мошенничества с использованием электронных средств платежа. Описаны обстоятельства, подлежащие установлению и доказыванию при совершении данных видов мошенничества.

Ключевые слова: *мошенничество; онлайн-платежи; интернет-технологии; электронные средства платежа; киберпреступность.*

Мошенничество в сфере электронной коммерции с онлайн-платежами – одно из наиболее распространенных видов мошенничества, которое обозначает любые незаконные онлайн-транзакции, совершаемые киберпреступниками. Жертва, как правило, – онлайн-пользователь, который испытывает следующие типы убытков: потеря денег, процентов, конфиденциальной информации или личного имущества через онлайн-средства.

С увеличением количества онлайн-транзакций и неограниченного доступа к интернет-технологиям онлайн-клиенты сталкиваются с множеством рисков для своей личной информации и нарушением политик безопасности. Еще одна серьезная проблема с системами онлайн-платежей – это управление мошенническими записями. Высокий спрос и предпочтения

пользователей в электронных транзакциях привели к активному развитию новых мошеннических методов. Поскольку мошенничество с онлайн-платежами является проблемой глобального масштаба, меры по борьбе с этим должны быть соразмерными [3].

Мошенничество с электронными платежами можно разделить на две категории: онлайн-мошенничество и офлайн-мошенничество. Кража или неправомерное использование важных учетных данных (личный идентификационный номер, данные кредитной карты), фишинг и спуфинг-атаки – все это различные типы онлайн-мошенничества. Примеры офлайн-мошенничества включают в себя вымогательство по телефону или мошенничество с использованием почты. По сравнению с ежегодным темпом роста транзакций, обнаружение и предотвращение такого мошенничества практически невозможно из-за его сложности и короткого периода времени, в течение которого транзакции происходят между двумя или более людьми [1].

Мошенничество с онлайн-платежами не ограничивается традиционным видом мошенничества, который известен как мошенничество с электронной почтой. Сегодня, когда Интернет широко распространен, используются различные методы и технологии, которые более развиты. Во всем мире почти каждый третий потребитель становится жертвой мошенничества с платежными картами. Согласно новым глобальным эталонным данным от «ACI Worldwide» и «AiteGroup», 30% потребителей во всем мире сталкивались с мошенничеством с картами за последние пять лет. Исследование глобального мошенничества, в котором приняли участие более 6000 потребителей в 20 странах, показало, что, по сравнению с исследованием 2018 г., посвященным показателям мошенничества с картами, незаконная деятельность по различным платежным картам (дебетовым, кредитным и предоплаченным) растет во всем мире. В период с 2018 по 2021 гг. количество случаев мошенничества с онлайн-платежами увеличилось на 280%. В России с начала прошлого года официально зарегистрированных преступлений, совершаемых с помощью Интернета, возросло до 300 тыс. [6].

Если рассматривать потенциальную жертву, то можно обратить внимание на некоторые виды поведения пользователей, которые могут оказаться рискованными, например, если оставить смартфон разблокированным. Это имеет прямую корреляцию с мошенничеством, так что ландшафт риска мошенничества с онлайн-платежами растет вместе с глобальным сдвигом в увеличении использования смартфонов/планшетов. С такими существующими лазейками в системе, касающейся платежных систем или онлайн-транзакций, преступники будут соблазнены их использовать.

Однако не только потребители подвергаются риску обнаружения мошенничества в Интернете. Недавние данные показывают, что у крупных розничных торговцев увеличивается количество случаев мошенничества по электронной почте, поскольку их предприятия подвергаются риску мошенничества с использованием электронной почты и онлайн-платежей. Меры предосторожности в отношении безопасности в Интернете, применяемые к потребителям, также могут защитить различные предприятия. Но в то же время для бизнеса также важно иметь план безопасности, чтобы сотрудники могли защитить конфиденциальные данные. У компаний должен быть ИТ-отдел, занимающийся защитой данных компании от незаконных групп, таких как хакеров или действий, при этом соблюдая все необходимые меры предосторожности [5].

Рассмотрим несколько распространенных методов мошенничества с использованием электронных средств платежа.

Кража личных данных. Некоторые из наиболее распространенных типов обнаружения онлайн-мошенничества – это кража личных данных, фишинг и кража учетной записи. Это может включать использование кредитных карт, поскольку мошенники могут легко провести транзакцию без предъявления карты. Кража личных данных не является чем-то новым,

поскольку она существует и за пределами цифрового мира [2]. Это тип мошенничества, в котором обычно участвует киберпреступник – тот, кто пытается украсть личную информацию клиента/пользователя, взломав их системы. После этого хакер использует эту информацию для незаконных транзакций онлайн-платежей. Поскольку киберпреступники обладают всей личной информацией клиентов, это позволяет им легко обходить любые брандмауэры или ограничения для обнаружения мошенничества. Однако поскольку вебсайт электронной коммерции не знает разницы и ошибочно принимает человека, совершающего покупку, как первоначального владельца кредитной карты, оплата производится легко. В большинстве этих сценариев большую часть предметов покупает хакер.

Фишинг. Существует множество вебсайтов и подписок по электронной почте, которые побуждают пользователя выбирать информационные бюллетени и предупреждения. В большинстве случаев эти подписки требуют от пользователя предоставления некоторых своих личных данных, включая данные кредитной карты. Если электронное письмо не из надежного источника, данные пользователя будут украдены и использованы для совершения незаконных транзакций. Чтобы этого не происходило, поисковые системы и веб-инструменты позволили пользователю идентифицировать надежные источники (банки, зарегистрированные предприятия и т.д.). Таким образом, они могут гарантировать, что их данные будут в надежных руках [3].

Расширенное мошенничество с банковским переводом и переводом комиссионных. При огромном пространстве Интернета есть вероятность, что человек может натолкнуться на поддельные сайты, запрашивающие небольшую сумму первоначального взноса, которую они обещают вернуть после того, как первоначальный платеж будет произведен. Это метод, с помощью которого хакеры-мошенники обманывают пользователей, заставляя их выдать данные своих кредитных карт. Хакеры хотят, чтобы клиенты завершили платеж за услугу или продукт, которые являются ложными, с помощью авансового денежного перевода – до того, как произойдет обнаружение мошенничества с платежами.

Мошенничество с идентификацией продавца – это тип мошенничества с онлайн-платежами, при котором киберпреступник создает торговую учетную запись, аналогичную учетной записи легального бизнеса. Затем преступник предъявляет ложные обвинения по кредитным картам, и все они украдены. Этот вид мошенничества совершается так быстро, что первоначальный держатель карты далек от понимания того, что произошло.

Pagejacking: сайты электронной коммерции / онлайн-бизнеса становятся мишенью для киберпреступников, которые используют свои веб-сайты для перехвата клиентов и перенаправления их на ненадежный источник веб-сайта. Целью этого является то, что нежелательный веб-сайт, вероятно, будет содержать некоторые вредоносные программы, которые могут взломать системы безопасности веб-сайта и ложным образом захватить средства пользователей. Согласно ФЗ № 161 от 27.06.2011 г. «О национальной платежной системе», в котором говорится что электронное платежное средство – это средство или метод, позволяющий клиенту компании по переводу денежных средств создавать, подтверждать и передавать распоряжения для перевода денежных средств в соответствии с применимыми формами безналичного расчета при использовании информационных и коммуникационных технологий, электронных носителей, в том числе платежных карт, и других технических устройств. Операторами денежных переводов являются Банк России, кредитные организации, уполномоченные осуществлять переводы денежных средств. Оператор электронных денег – это кредитная организация, которая является небанковской кредитной организацией и уполномочена осуществлять денежные переводы без открытия банковских счетов и другие связанные банковские операции.

Денежные средства в настоящее время делятся на наличные, безналичные и электронные. Необходимость в переводе денег и размещении переводных поручений существует только в случае безналичных и электронных денег, поскольку только эти виды денег нуждаются в обязательном участии посредников между субъектами расчетов – трансферных компаний, которым поданы поручения на перевод отправлений безналичных или электронных денег.

Непосредственным объектом мошенничества с электронными платежами является собственность определенных физических и юридических лиц, о чем говорится в гл. 21 УК РФ, в котором закреплено рассматриваемое нами преступление.

Одна из основных проблем в понимании признаков мошенничества – правильное установление предмета преступного вмешательства. В случае мошенничества это собственность, с одной стороны, и право собственности – с другой. Все чаще поднимается дискуссия, которая относит предмет мошенничества к имущественным правам, отличным от прав собственности. Термин «приобретение прав на собственность третьих лиц» трактовался в уголовном праве в значительной степени ограничительно. Присвоение права собственности субъекту преступления вызывает возражения, поскольку у него еще нет собственности, на которую лицо приобрело такое право. Приобретение права позволяет человеку вступать во владение или распоряжаться чужой собственностью, как своей. Что касается права использования, то оно позволяет преступнику использовать собственность и извлекать из нее полезные свойства, не превращая само имущество в собственность преступника.

Предметом уголовного преступления по ст. 159.3 УК РФ некоторые ошибочно определяют платежную карту. Однако сама платежная карта не имеет стоимости. Мошенники пытаются завладеть ими, чтобы получить доступ к средствам, которые находятся на счетах, привязанных к платежным картам.

Итак, проблема мошенничества с платежными картами – это деньги.

Мошенничество может быть тотальным как в отношении физического лица (держателя платежной карты), так и в отношении юридического лица (держателя банковского или иного счета).

Считается, что среда, в которой происходит мошенничество с платежными картами, во многом будет зависеть от выбранного типа мошенничества. Классифицировать мошенничество через Интернет можно следующим образом: через интернет-магазины и различные сайты с объявлениями о продаже и оказания услуг, мобильный телефон («тревожные звонки») и электронное мошенничество через банкоматы – «скимминг». Совершают данное преступление преимущественно мужчины в возрасте от 16 до 39 лет – 83,9% и только 16,1% – женщины. Уровень образования: среднее – 38%, среднее специальное – 31%, высшее – 11%.

Способ совершения мошенничества и злоупотребление доверием – это формы мошенничества с использованием электронных платежных средств.

На основании определения мошенничества в постановлении Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» можно сделать вывод, что при использовании данного метода в случае кражи необходимо взаимодействие субъекта с потерпевшим или другим лицом, в результате чего не существует коммерческой тайны преступника. Преступник влияет на сознание и волю другого человека. Кража денежных средств путем снятия средств из банкомата с банковской картой, незаконно находящейся у лица, является составом преступления (п. «Г» части 3 статьи 158 УК РФ).

Злоупотребление доверием – второй способ совершения рассматриваемого преступления – это форма обмана и, следовательно, возможна только между людьми. Уполномоченный сотрудник кредитной, коммерческой или иной организации – это лицо, которое имеет трудовые или иные отношения с такой организацией и которое уполномочено прово-

дить расчетные операции со средствами с использованием платежных карт от имени и в интересах этой организации (кассовый аппарат, продавец и т.д.). По мнению некоторых авторов, применение данной концепции не совсем корректно, поскольку возникает вопрос об обмане «неуполномоченного сотрудника».

Рассмотрим средство совершения преступления. Поддельная кредитная, дебетовая или другая платежная карта, полученная кем-то еще, является средством совершения преступления. Банковская карта не может быть объектом имущественных преступлений, поскольку не имеет экономической ценности. Остается неясным вопрос о содержании термина «электронное платежное средство». Определение электронного платежного средства содержится в Федеральном законе от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе». Согласно п. 19 ч. 1 ст.3 настоящего Закона электронным средством платежа является средство и (или) способ, позволяющий клиенту компании по переводу денежных средств передавать поручения на перевод денежных средств в рамках применяемых форм безналичных платежей с использованием информационно-коммуникационных технологий, электронных носителей, включая платежные карты, а также других технических устройств. Платежные карты – это первый в мире самый популярный способ электронных платежей. ЦБ РФ определил виды платежных карт в зависимости от условий расчетов между эмитентом карты и ее держателем: кредитные, платежные и предоплаченные карты.

Способы совершения мошенничества с использованием электронных средств платежа: обман злоумышленником уполномоченного сотрудника организации путем предоставления ему поддельной платежной карты с последующим выводом средств, оплатой товаров и услуг; злоумышленник обманул уполномоченного сотрудника организации, предоставив ему украденную платежную карту с последующим выводом денежных средств и оплатой товаров и услуг; преступление совершено группой лиц по предварительному сговору; использовано свое служебное положение.

Одним из идеальных следов рассматриваемого преступления является описание явки преступника свидетелями, потерпевшими. К материальным следам преступления относятся документы, в том числе электронные, подтверждающие факт перечисления денег со счета (чека), снятие наличных (договор между держателем карты и кредитной организацией, выписка из банка и т.д.).

Обстоятельства, подлежащие установлению и доказыванию, включают в себя [1]:

- наличие корыстной цели, стремления изъять и (или) обратить чужое имущество в свою пользу либо распорядиться им как своим собственным, в том числе путем передачи его в обладание других лиц, круг которых не ограничен;

- каким способом было совершено хищение чужого имущества или права на чужое имущество – путем обмана или злоупотребления доверием, под воздействием которых владелец имущества или иное лицо передали имущество или право на него другому лицу, либо не препятствуя изъятию этого имущества или приобретению права на него другим лицом;

- в чем именно состоял обман как способ совершения преступления, предусмотренного ст. 159.3 УК РФ: в сознательном сообщении либо представлении заведомо ложных, не соответствующих действительности сведений либо в умолчании об истинных фактах, либо умышленных действиях, направленных на введение владельца в заблуждение. Например, в предоставлении фальсифицированного товара или иного предмета сделки, использовании различных обманных приемов при расчетах за товары или услуги, имитации кассовых расчетов и т.д.;

- какие именно сведения были сообщены или скрыты злоумышленником;

- использовался ли обман для непосредственного завладения чужим имуществом;

- намеревался ли злоумышленник исполнять обязательства, связанные с объектом преступления. Наличие причинно-

следственной связи с причиненным потерпевшему ущербом;

- в случае совершения мошенничества с использованием электронных средств платежа группой лиц необходимо установить роль каждого в совершении всех эпизодов преступной деятельности;

- установление точной суммы ущерба. В случае, если сумма ущерба не превышает 2500 руб., а виновный является лицом, подвергнутым административному наказанию за мелкое хищение чужого имущества стоимостью более одной тысячи рублей, но не более 2500 руб., и в его действиях отсутствуют признаки преступления, предусмотренные ч.ч. 2, 3, 4 ст. 159.3 УК РФ, то деяние подлежит квалификации по ст. 158.1 УК РФ;

- установление факта причинения значительного ущерба не только посредством установления суммы причиненного ущерба, но и путем исследования имущественного положения потерпевшего (наличие источника доходов, их размер и периодичность поступления, наличие иждивенцев, совокупный доход членов семьи, с которыми он ведет совместное хозяйство), а также мнение потерпевшего о значительности причиненного ущерба;

- установление факта причинения крупного и особо крупного размера ущерба для п.п. 3 и 4 ст. 159.3 УК РФ согласно общему правилу, регламентированному п. 4 примечания к ст. 158 УК РФ;

- установление места и момента (точного времени) изъятия денежных средств с банковского счета их владельца или электронных денежных средств, в результате которого владельцу этих денежных средств причинен ущерб.

Таким образом, криминалистические признаки правонарушения, согласно ст. 159.3 УК РФ, достаточно разработаны и способствуют полному и всестороннему расследованию мошенничества с целью привлечения виновных к ответственности.

ЛИТЕРАТУРА

1. *Анешева А.Т.* Обстоятельства, подлежащие установлению по делам о кражах, совершенных с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного статьей 159.3 УК РФ) / А.Т. Анешева. – Текст: непосредственный // Законодательство и практика. – 2021. – № 1. – С. 41–44.

2. *Кирилловых А.А.* Электронные средства платежа: проблемы гражданско-правовой природы и уголовно-правовой охраны / А.А. Кирилловых, Д.А. Овсюков. – Текст: непосредственный // Право и экономика. – 2019. – № 1. – С. 62–70.

3. *Курбатов А.Я.* Неперсонифицированные электронные средства платежа: порядок и проблемы использования / А.Я. Курбатов. – Текст: непосредственный // Банковское право. – 2019. – № 2. – С. 46–51.

4. *Орловский Е.А.* К вопросу о противодействии хищениям, совершенным с использованием электронных средств платежа / Е.А. Орловский. – Текст: непосредственный // Российская юстиция. – 2020. – № 6. – С. 24–26.

5. *Скрипченко Н.Ю.* Уголовная ответственность за хищения денежных средств с банковского счета (анализ законодательных новелл) / Н.Ю. Скрипченко. – Текст: непосредственный // Банковское право. – 2020. – № 1. – С. 44–49.

6. *Тюнин В.И.* Кража с банковского счета, а равно в отношении электронных денежных средств (криминализация и квалификация преступления) / В.И. Тюнин, Ю.И. Степанов. – Текст: непосредственный // Российский следователь. – 2021. – № 3. – С. 41–45.