УДК 343.98.062

Вновь о способах мошенничеств, совершаемых с использованием средств телефонной связи, и механизме следообразования

Машлякевич Вячеслав Андреевич

Старший преподаватель кафедры огневой и технической подготовки,
Барнаульский юридический институт Министерства внутренних дел Российской Федерации,
656039, Российская Федерация, Барнаул, ул. Чкалова, 49;
e-mail: basistoo87@gmail.com

Аннотация

Автор рассматривает относительно новый способ совершения мошенничества с использованием средств телефонной связи. Преступник находит потенциального потерпевшего по размещенному им объявлению о продаже какого-либо имущества на специализированном сайте. Введя потерпевшего в заблуждение, он осуществляет привязку принадлежащей ему банковской карты к своему номеру телефона, после чего совершает похищение находящихся на ней денежных средств. В статье на основе эмпирического материала определены критерии выбора таких объявлений преступником, подробно и последовательно приведены его действия на протяжении всего преступления. Кроме того, автор уделяет внимание механизму следообразования при совершении рассматриваемого вида мошенничества предлагаемым способом. Каждая группа следов (идеальные, материальные, электронно-цифровые) подробно описана с указанием на их источник.

Для цитирования в научных исследованиях

Машлякевич В.А. Вновь о способах мошенничеств, совершаемых с использованием средств телефонной связи, и механизме следообразования // Вопросы российского и международного права. 2019. Том 9. № 7А. С. 209-214.

Ключевые слова

Мошенничество, телефонное мошенничество, следообразование, механизм следообразования, обман с использованием средств связи.

Введение

Одной из насущных проблем, вставших в последнее время перед правоохранительными органами, является проблема раскрытия и расследования мошенничеств, совершаемых с использованием средств телефонной связи. Стремительное развитие данный вид преступной деятельности получил в 2009-2015 гг., однако и по настоящее время объемы совершаемых преступлений подобного рода не снижаются. Так, за 2018 г. выявлено 9700 преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий, что на 12,6% больше, чем за 2017 г. [Состояние преступности, www]. Предпринимаемые органами внутренних дел попытки профилактической работы дают некоторые положительные результаты, однако они же становятся своеобразным катализатором совершенствования преступного мира. Так, способы, с помощью которых совершались телефонные мошенничества пять лет назад, постепенно отходят на второй план, уступая пальму первенства новым вариациям.

Описание наиболее традиционных видов совершения мошенничеств с использованием средств телефонной связи можно встретить в достаточно большом количестве публикаций, касающихся криминалистических и оперативно-розыскных аспектов раскрытия и расследования преступлений [Ермаков, 2018; Гилязов, 2014; Качановский, 2014]. Подавляющее большинство авторов упоминает такие способы, как «Ваш родственник попал в беду» и «Ваша банковская карта заблокирована», что вполне логично, так как они являются наиболее распространенными. Вместе с тем в последнее время набирают популярность другие варианты, с помощью которых телефонные мошенники похищают денежные средства. Речь идет об использовании в преступных целях объявлений граждан о продаже их имущества, размещаемых на различных интернет-площадках (Avito.ru, Drom.ru и т. п.).

Особенности рассматриваемого способа совершения мошенничества с использованием средств телефонной связи

Существует две внешне схожих схемы их использования преступниками – звонок по объявлению добропорядочного гражданина и размещение «объявления-приманки», по которому будут обращаться добропорядочные граждане. Анализ уголовных дел показал, что гораздо чаще (около 84% случаев) мошенник использует первый вариант в своей преступной деятельности, поэтому остановимся на нем подробнее.

Полагаем верным считать, что рассматриваемый вид преступления берет свое начало с момента осуществления злоумышленником поиска на специализированных интернет-сайтах подходящих объявлений о продаже личного имущества граждан. Основным критерием отбора таких объявлений, как правило, является стоимость продаваемого объекта. Он не должен быть слишком дешевым (например, мошенника не заинтересует объявление о продаже одежды за 500-1000 рублей), однако и не должен быть слишком дорогим (автомобиль стоимостью в 500 000 рублей также не привлечет внимания преступника). Как показывает анализ уголовных дел по преступлениям рассматриваемой категории, диапазон стоимости имущества, продаваемого гражданами на интернет-сайтах, которое входит в сферу интересов мошенников, варьируется от 10 000 до 200 000 рублей.

Преступник, подобрав подходящее объявление, осуществляет телефонный звонок его автору с предложением немедленной покупки продаваемого. При этом следует отметить, что наибольшей популярностью у мошенников пользуются такие объявления, после размещения

которых прошло как можно меньшее количество времени. Это создает дополнительное психологическое воздействие на продавца, которому не терпится продать свое имущество. В ходе телефонного разговора злоумышленник выясняет состояние вещи (либо объекта), как долго ей (им) пользовались и т. п., так как автором объявления о продаже он должен восприниматься как действительно заинтересованный покупатель. В дальнейшем мошенник предлагает купить указанное в объявлении имущество путем безналичного расчета – перевода денежных средств на банковскую карту продавца. Для этого он направляет продавца к банкомату. В некоторых случаях, с целью разыгрывания более правдивой ситуации, преступник прерывает разговор с потенциальным потерпевшим, выжидает некоторое время (5-10 минут) и, перезвонив, сообщает, что перевести денежные средства за продаваемое имущество со своей банковской карты ему не удалось. Для проведения такой операции он просит пройти продавца к банкомату, чтобы тот «подтвердил получение денежных средств».

Последующие действия преступника сводятся к тому, что он путем обмана заставляет потерпевшего привязать свою банковскую карту к указанному им номеру телефона. Получив таким образом доступ к денежным средствам, злоумышленник переводит их на балансы различных сим-карт, электронных кошельков либо банковских карт по своему усмотрению[1].

Следует отметить, что мошенник заранее продумывает ответы на возможные вопросы потерпевшего, оказывает на него психологическое воздействие путем постоянных разговоров о предмете сделки, не давая тем самым опомниться и прервать свои действия по «приему оплаты за продаваемое имущество».

Особенности механизма следообразования рассматриваемого способа совершения мошенничества с использованием средств телефонной связи

Механизм следообразования при данном способе совершения мошенничества с использованием средств телефонной связи будет выражаться по большей своей части в электронно-цифровых следах, отобразившихся на различных устройствах, используемых преступником и потерпевшим [Машлякевич, 2014].

Как уже упоминалось, первоначальным действием злоумышленника будет поиск объявления о продаже имущества. Такой поиск можно осуществить посредством смартфона, имеющего доступ к сети Интернет, а также компьютерной техники (нетбука, ноутбука, планшетного компьютера и т. д.), которая также должна иметь доступ к сети Интернет. Соответственно, на устройстве, с которого был осуществлен поиск подходящего объявления, останутся следы поисковых запросов, посещения веб-страницы с конкретным объявлением о продаже, интересующим следователя.

Следующим шагом преступника является звонок потерпевшему с предложением покупки его имущества. Для этого мошенник будет использовать мобильный телефон, на корпусе которого, а также на сим-карте, флэш-карте и аккумуляторной батарее могут быть обнаружены микрочастицы, запаховые и потожировые следы человека, следы механических повреждений, а также пальцев рук. В списке исходящих вызовов останутся данные о набранном номере, а также (в зависимости от модели телефона) будут указаны время осуществления звонка и длительность вызова. Известно, что каждый телефон имеет уникальный для него международный

1 См., например, обвинительное заключение СЧ СУ УМВД России по г. Новокузнецку по уголовному делу № 16140111 от 27 января 2017 г.

идентификатор мобильного оборудования – IMEI, благодаря которому информация о звонках и смс-сообщениях отражается в информационных системах операторов сотовой связи. По соответствующему запросу в рамках расследуемого уголовного дела следователь может получить сведения об абонентах персональных идентификационных карт, используемых в сотовом телефоне преступника, а также сведения о соединениях по абонентскому номеру с указанием базовых станций. Фактически те же электронно-цифровые следы можно обнаружить и при исследовании мобильного телефона потерпевшего.

Не стоит пренебрегать и идеальными следами преступления. Так, потерпевший может запомнить и впоследствии опознать голос преступника. Также носителями идеальных следов могут быть лица, случайным образом засвидетельствовавшие момент совершения преступления. Как правило, ими являются сокамерники преступника, отбывающие с ним наказание в исправительном учреждении.

Например, допрошенный в качестве свидетеля Л. показал, что содержится в СИЗО-1 г. Новосибирска. В последних числах декабря 2013 г. в камеру был помещен Р., который привез с собой мобильный телефон. В первых числах января Л. услышал, как Р., находясь в камере, стал осуществлять телефонные звонки незнакомым ему гражданам с целью получения денежных средств, т. е. совершать телефонное мошенничество[2].

Последующие действия преступника касаются процесса привязки банковской карты потерпевшего к номеру телефона, указанному преступником. Напомним, что для этого мошенник под разными предлогами отправляет потерпевшего к банкомату, где, следуя инструкциям, последний осуществляет перерегистрацию мобильного номера телефона. Используя эту информацию, следователю необходимо получить записи с камер видеонаблюдения, установленных в отделении банка, которое посетил потерпевший. Кроме того, если преступление происходило в рабочее время, то необходимо опросить сотрудников банка, работавших в качестве консультантов зала обслуживания клиентов. Также следует запросить запись камеры, установленной непосредственно на банкомате, которым пользовался потерпевший. Материальным следом на данном этапе будет являться чек, полученный потерпевшим из банкомата, на котором отображена информация об идентификаторе пользователя и пароле для входа в систему «Сбербанк Онлайн».

Электронно-цифровые следы, отображающие факт использования банковской карты потерпевшим в определенное время и в определенном банкомате, содержатся в банковских информационных системах. Кроме того, там же отображается информация о номерах мобильных телефонов, привязанных к банковской карте. Другой вид электронно-цифровых следов на данном этапе совершения мошенничества возникнет в мобильном телефоне преступника – это смс-сообщение о том, что определенная банковская карта привязана к его номеру телефона.

Дальнейший этап – перевод мошенником денежных средств с банковской карты (нескольких карт, вкладов и т. п.) потерпевшего на баланс сим-карт мобильных телефонов, других банковских карт, электронные кошельки, к которым преступник каким-либо образом имеет доступ (сам либо через доверенное лицо). Все факты движения денежных средств любым упомянутым способом отображаются в соответствующем программном обеспечении, имеющемся в банках, компаниях сотовой телефонной связи, компаниях – владельцах

2 См. обвинительное заключение СО межмуниципального отдела МВД России «Барабиинский» Новосибирской области по уголовному делу № 460206 (2014 г.).

электронных кошельков. Такие сведения следователь может истребовать, направив соответствующие запросы в рамках расследуемого уголовного дела.

Заключение

Таким образом, вновь изобретаемые мошенниками способы совершения преступлений с использованием средств телефонной связи неизменно влекут за собой появление новой следовой картины. Процессы движения денежных средств, отображающиеся как в мобильных телефонах преступника и потерпевшего, так и в информационных системах банковских организаций, компаний сотовой телефонной связи, компаний – владельцев электронных кошельков, играют существенную роль в раскрытии и расследовании данного вида преступной деятельности, так как несут в себе достаточно объемный массив следовой информации. Ее получение в процессе расследования уголовного дела по рассматриваемой категории преступлений предполагает активную деятельность лица, проводящего расследование, по подготовке большой массы запросов в различные организации. Полноценный сбор рассмотренных нами следов мошенничества, совершаемого с использованием средств телефонной связи, несомненно, способствует проведению качественного расследования данной категории преступлений.

Библиография

1. Гилязов Р.Р. Способы совершения мошенничеств с использованием средств сотовой телефонной связи как элемент криминалистической характеристики // Евразийский юридический журнал. 2014. № 21. С. 167-169.
2. Ермаков С.В. Особенности оперативно-розыскной характеристики мошенничеств, совершаемых с использованием средств сотовой связи // Материалы XVI Международной научно-практической конференции «Актуальные проблемы борьбы с преступлениями и иными правонарушениями». Барнаул, 2018. Ч. 1. С. 21-23.
3. Качановский А.С. Квалификация телефонного мошенничества // Законность. 2014. № 5. С. 50-53.
4. Машлякевич В.А. Некоторые аспекты механизма следообразования при расследовании мошенничеств, совершаемых с использованием средств телефонной связи // Мир юридической науки. 2014. № 1-2. С. 51-57.
5. Состояние преступности. URL: https://мвд.рф/folder/101762/

Again on the ways of committing fraud through means of telephone communication and the mechanism of trace formation

Vyacheslav A. Mashlyakevich

Senior Lecturer at the Department of fire and technical training,
Barnaul Law Institute of the Ministry of Internal Affairs of the Russian Federation,
656039, 49, Chkalova st., Barnaul, Russian Federation;
e-mail: basistoo87@gmail.com

Abstract

The article examines a relatively new way of committing fraud through means of telephone communication. A criminal finds a potential victim by looking through property sale announcements posted on specialised sites. By misleading the victim, he/she binds the victim's bank card to his/her phone number, and then steals the money. The author of the article uses empirical material to identify

the criteria for choosing such announcements by criminals, describes their actions in the process of committing fraud through means of telephone communication. The article pays attention to the mechanism of trace formation in the commission of this type of fraud and describes in detail each group of traces (ideal, material, digital). The newly invented ways of committing fraud through means of telephone communication invariably entail the emergence of a new trace pattern. In order to collect evidence in the course of investigation of such a criminal case in the proper way, an investigator sends a lot of letters of inquiry to various organisations, including banking organisations, cellular telephone companies and digital wallet companies. The full collection of the traces of fraud committed through means of telephone communication, undoubtedly, contributes to the careful and thourough investigation of this category of crimes.

For citation

Mashlyakevich V.A. (2019) Vnov' o sposobakh moshennichestv, sovershaemykh s ispol'zovaniem sredstv telefonnoi svyazi, i mekhanizme sledoobrazovaniya [Again on the ways of committing fraud through means of telephone communication and the mechanism of trace formation]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 9 (7A), pp. 209-214.

Keywords

Fraud, telephone fraud, trace formation, mechanism of trace formation, deception through communication means.

References

1. Ermakov S.V. (2018) Osobennosti operativno-rozysknoi kharakteristiki moshennichestv, sovershaemykh s ispol'zovaniem sredstv sotovoi svyazi [The features of the operational-search characteristics of fraud committed through means of cellular communication]. *Materialy XVI Mezhdunarodnoi nauchno-prakticheskoi konferentsii "Aktual'nye problemy bor'by s prestupleniyami i inymi pravonarusheniyami"* [Proc. 16th Int. Conf. "Topical problems of combating crimes and other offences"], Part 1. Barnaul, pp. 21-23.
2. Gilyazov R.R. (2014) Sposoby sovershenia moshennichestv s ispol'zovaniem sredstv sotovoi telefonnoi svyazi kak element kriminalisticheskoi kharakteristiki [Ways to commit fraud through means of cellular communication as an element of forensic characteristics]. *Evraziiskii yuridicheskii zhurnal* [Eurasian law journal], 21, pp. 167-169.
3. Kachanovskii A.S. (2014) Kvalifikatsiya telefonnogo moshennichestva [Legal assessment of telephone fraud]. *Zakonnost'* [Legality], 5, pp. 50-53.
4. Mashlyakevich V.A. (2014) Nekotorye aspekty mekhanizma sledoobrazovaniya pri rassledovanii moshennichestv, sovershaemykh s ispol'zovaniem sredstv telefonnoi svyazi [Some aspects of the mechanism of trace formation in the investigation of fraud committed through means of telephone communication]. *Mir yuridicheskoi nauki* [The world of legal science], 1-2, pp. 51-57.
5. *Sostoyanie prestupnosti* [The state of crime]. Available at: https://mvd.rf/folder/101762/ [Accessed 18/06/19].