УДК 343.721

ТИПИЧНЫЕ СЛЕДСТВЕННЫЕ ДЕЙСТВИЯ В РАМКАХ МЕТОДИКИ РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ И СРЕДСТВ МОБИЛЬНОЙ СВЯЗИ

TYPICAL INVESTIGATIONS IN THE FRAMEWORK OF THE FRAUD INVESTIGATION METHOD WITH USING THE INTERNET NETWORK AND MOBILE COMMUNICATION FACILITIES

©Лаврушкина А. А.,
Национальный исследовательский Мордовский
государственный университет им. Н. П. Огарева,
г. Саранск, Россия, lawr88alina@yandex.ru
©Lavrushkina A.,
Ogarev Mordovia State University,
Saransk, Russia, lawr88alina@yandex.ru

Аннотация. В статье рассмотрена специфика расследования мошенничества с использованием сети Интернет и средств мобильной связи. Приведены примеры типичных следственных действий. Проанализированы проблемы расследования, причины затягивания следствия, которые исходят из специфики совершаемого преступления. С учетом положений ведомственных нормативных актов изложена позиция относительно места окончания мошенничества с использованием сети Интернет.

Abstract. The article examines the specifics of the investigation of fraud using the Internet and mobile communications. Examples of typical investigative actions are given. The problems of the investigation, the reasons for delaying the investigation, which is based on the specifics of the crime being committed, are analyzed. Taking into account the provisions of departmental normative acts, the position regarding the place of termination of fraud using the Internet is stated.

Ключевые слова: мошенничество, расследование, сеть Интернет, следственные действия, следствие, средства мобильной связи.

Keywords: fraud, investigation, Internet network, investigative actions, investigation, means of mobile communication.

В XXI веке мошенничество приобретает новую форму, которая соответствует духу информационных и компьютерных технологий. Распространение интернет-банкинга, электронных платежей, привело к тому, что злоумышленники стали активно использовать достижения научно-технического прогресса при совершении преступлений. Основные средства, используемые при совершении мошеннических действий, связаны с использование Интернета, а также компьютера и мобильных средств связи.

Подобные факты мошеннических действий именуют по-разному, нередко называют «дистанционным мошенничеством» [3], наиболее распространенной формулировкой является «мошенничество с использованием сети Интернет и средств мобильной связи» (3). Не углубляясь в тонкости наименования данного вида мошенничества, так как механизм

действий от этого никак не меняется, отметим особенности методики расследования рассматриваемого деяния.

Отметим, что для следственной практики факты мошенничества с использованием сети Интернет и средств мобильной связи являются далеко не самой простой категорий дел. Чаще всего возбужденное дело не доходит до судебного разбирательства, так как расследование подобных преступлений приходит в тупик и следствие приостанавливается по п. 1 ч. 1 ст. 208 УПК РФ (1), то есть в связи с отсутствием лица, подлежащего привлечению в качестве обвиняемого. Иными словами, данную категорию дел можно назвать обыденной для следственных органов терминологией — «глухарями».

Подобная ситуация обусловлена трансграничностью рассматриваемого вида мошенничества, отсутствием четкой определенности относительно места окончания преступления, достоверной информации о принадлежности абонентских номеров, данных банковских карт, сведений о том, на какой счет были перечислены денежные средства потерпевшим. Иногда вышеназванные сведения не представляется возможным установить, так как соответствующие данные не сохраняются, либо они недостоверные, принадлежат вымышленным лицам или гражданам, которые вообще не причастны к совершению преступления. Поэтому круг эффективных оперативно-розыскных средств и методов не так широк.

Как правило, когда поступает сообщение о фактах мошеннических действий подобного характера, предварительно проводится проверка сообщения о преступлении, до возбуждения уголовного дела. И на этом этапе возникает немало вопросов относительно места окончания преступления, а следовательно, и о территориальной подследственности.

Ситуация складывается двояко, когда местом окончания преступления считают место перевода потерпевшим денежных средств, либо преступление считают оконченным в месте, где виновный похитил денежные средства. На практике это приводит к переписке органов предварительного расследования между собой по вопросам определения территориальной подследственности, что необоснованно затягивает производство по уголовному и негативно сказывается на результатах расследования в целом. Складывается ситуация, когда материал предварительной проверки блуждает между различными отделами полиции в рамках одного, а чаще всего между различными субъектами нашей страны.

Для единообразия следственной практики существует ряд ведомственных актов, которые призваны сориентировать правоприменителей относительно места окончания преступления.

Так в 7 пункте Приказа Генеральной прокуратуры РФ, МВД РФ, МЧС РФ, Минюста РФ, ФСБ РФ, Минэкономразвития РФ и Федеральной службы РФ по контролю за оборотом наркотиков от 29 декабря 2005 г. №39/1070/1021/253/780/353/399 «О едином учете преступлений», указано, что в случае, если не представляется возможным определить место совершения преступления, оно подлежит учету по месту его выявления (2).

Врио Министра внутренних дел Российской Федерации Горовой А. В., который в своем письме от 13.07.2015 №1/5562 «Об организации работы по противодействию отдельным видам мошенничества», указывал на то, что, при поступлении заявления (сообщения) о совершении мошеннических действий с использованием мобильных средств связи, осуществлять проверку и при наличии в деянии признаков преступления принимать решение о возбуждении уголовного дела территориальным органом, принявшим заявление либо иное сообщение. При этом в случае установления в ходе расследования точного места совершения преступления за пределами обслуживаемой территории после производства неотложных

следственных действий направлять уголовное дело по подследственности в порядке, установленном статьей 152 УПК РФ [1].

То есть в данном случае ответ однозначный, если невозможно определить место окончания преступления, то расследовать необходимо по месту выявления.

В рамках доследственной проверки, а также впоследствии при производстве по уголовному делу оперативными работниками, следователями производится ряд типичных оперативно-розыскных мероприятий и следственных действий.

Изначально направляется ряд запросов в зависимости от обстоятельств дела в различные организации, регистрирующие интернет-кошельки (Яндекс Деньги, Киви-банк и др.) с целью получения анкетных данных клиентов при регистрации кошелька, данные об IP адресах с которых производилось открытие кошелька.

Фактически всегда направляются запросы к операторам сотовой связи для истребования детализации данных абонентских номеров и установления принадлежности этих номеров, то есть анкетных данных лиц, на которых они были зарегистрированы.

Не остаются без внимания следователей и банки, куда также направляются запросы, относительно анкетных данных владельца счета, на который поступили денежные средства потерпевшего. Также банки по запросу следователей и оперативных работников могут предоставить информацию о движении денежных средств, а также документов касающихся, подключения услуги Мобильный банк.

Как правило, для получения вышеназванной информации требуется соответствующее разрешения суда, по каждой организации, куда направляется запрос, ибо чаще всего, необходимая следователем информация относится к охраняемой законом тайне и для получения доступа к ней, нужна соответствующая санкция суда.

Оперативные работники и следователи готовят соответствующие материалы для возбуждения перед судом ходатайства о получении информации о соединениях между абонентами и (или) абонентскими устройствами, а именно: о предоставлении разрешения на получение данных о входящих и исходящих соединениях, установлении IMEI-номера, с которым работала сим-карта, с указанием привязки к базовой станции ее адреса местоположения и азимута направления, о движении денежных средств по абонентскому номеру, на который были перечислены денежные средства, и о том, с какими IMEI-номерами работал абонентский номер в интересующий период времени и т. д. [2].

Вышеназванные запросы следователей очень часто остаются без ответа до того момента пока следственный орган не направит повторные запросы, а нередко и их бывает недостаточно. То есть складывается ситуация, когда операторы сотовой связи, а нередко и банки далеко не с первого раза реагируют на запросы соответствующих следственных органов.

Подобная нерасторопность вышеупомянутых организаций неминуемо тормозит сам процесс расследования и проверки сообщения о преступлении, так как отсутствие данных о том, на какой счет были перечислены денежные средства потерпевшего, владельце абонентского номера, банковской карты фактически делает следователей безоружными при расследовании мошенничества с использованием сети Интернет и средств мобильной связи.

Как и в рамках любого уголовного дела производится допрос потерпевших, свидетелей. Осуществляются выемка, осмотр соответствующих предметов (документов), с последующим их приобщением к материалам уголовного дела.

В случае установления каких-либо данных относительно лица, которому могли бы быть перечислены денежные средства потерпевшего, направляются поручения из органа

расследующего уголовное дело в другой орган следствия для допроса этого лица относительно причастности к совершенному преступлению. Эти мероприятия также затягивают производство предварительного расследования.

Однако проведенные оперативно-розыскные мероприятия и следственные действия не всегда дают положительный результат, так как очень часто абонентские номера зарегистрированы на лиц, не имеющих никакого отношения к обстоятельствам дела, а данные о владельцах банковских карт, на которые происходило списание денежных средств либо скрываются от следствия, либо опять же не причастны к событию, в связи с этим производство по делу приостанавливается.

В процессе расследования органы внутренних дел направляют в банк представление о необходимости принятия мер по установлению условий и способов совершения преступлений, проведения разъяснительных мероприятий с клиентами, например, относительно подключения услуги «Мобильный банк», а также о фактах мошеннических действий осуществляемых посредством этой услуги. Так как очень часто мошенничества с использованием сети Интернет и средств мобильной связи совершаются именно посредством услуги «Мобильный банк». Однако активная реклама банковских менеджеров данной услуги свидетельствует об игнорировании представлений органов внутренних дел.

Многочисленные рекомендации, адресованные гражданам со стороны органов внутренних дел, свидетельствуют о том, что для защиты от мошенничества с использованием сети Интернет и средств мобильной связи необходимо быть предельно внимательными и бдительными. Нужно достаточно критично относиться к любому роду сообщениям относительно блокировки банковской карты, присуждения выигрыша и т. д.

Источники:

(1). Уголовно-процессуальный кодекс Российской Федерации: ФЗ от 18.12.2001 №174-ФЗ // Собрание законодательства РФ. 2001. №52 (Ч. 1). Ст. 2921.

(2). Приказ Генеральной прокуратуры РФ, МВД РФ, МЧС РФ, Минюста РФ, ФСБ РФ, Минэкономразвития РФ и Федеральной службы РФ по контролю за оборотом наркотиков от 29 декабря 2005 г. N 39/1070/1021/253/780/353/399 «О едином учете преступлений».

(3). Официальный сайт МВД по Челябинской области Режим доступа: https://clck.ru/D9CtD. (дата обращения: 16.03.2018).

Sources:

(1). The Code of Criminal Procedure of the Russian Federation: FZ of 18.12.2001 №174-FZ // Collection of the legislation of the Russian Federation. 2001. №52 (Part 1). Art. 2921.

(2). Order of the Prosecutor General’s Office of the Russian Federation, the Ministry of the Interior of the Russian Federation, the Ministry of Emergency Situations of the Russian Federation, the Ministry of Justice of the Russian Federation, the Federal Security Service, the Ministry of Economic Development and the Federal Service for Drug Control of the Russian Federation no. 39/1070/1021/253/780/353/399 of December 29, 2005 a single account of crimes.

(3). Official site of the Ministry of Internal Affairs for the Chelyabinsk region. Access mode: https://clck.ru/D9CtD. (date of circulation: 16.03.2018).

Список литературы:

1. Аксенова Л. Ю. Алгоритм действий следователя и органа дознания при расследовании мошенничеств с использованием средств сотовой связи // Вестник Омской юридической академии. 2016. №3. 80-84.

2. Баранов С. А., Лазарев Д. С., Новикова Е. А., Волченко А. В. О некоторых вопросах определения территориальной подследственности по преступлениям, связанным с хищением денежных средств путем использования информационно-коммуникационных систем // Проблемы правоохранительной деятельности. 2017. №1. С. 67-70.

3. Литвинов Н. Д., Федоров А. Н. Мошенничество с использованием средств мобильной связи (дистанционное): понятие и особенности совершения // Научно-исследовательские публикации. 2015. №12. С. 73-80.

References:

1. Aksenova, L. Yu. (2016). Algorithm of the actions of the investigator and the body of inquiry in the investigation of frauds using mobile communication facilities. *Bulletin of the Omsk Law Academy,* (3). 80-84.

2. Baranov, S. A., Lazarev, D. S., Novikova, E. A., & Volchenko, A. V. (2017). About some questions of definition of territorial investigation on crimes connected with embezzlement of money resources by using information and communication systems. *Problems of law enforcement activity,* (1). 67-70.

3. Litvinov, N. D., & Fedorov, A. N. (2015). Fraud with the use of mobile communications (remote): the concept and features of the commission. *Scientific-research publications,* (12). 73-80.

Работа поступила
в редакцию 22.03.2018 г.

Принята к публикации
25.03.2018 г.

Ссылка для цитирования:

Лаврушкина А. А. Типичные следственные действия в рамках методики расследования мошенничества с использованием сети Интернет и средств мобильной связи // Бюллетень науки и практики. 2018. Т. 4. №4. С. 447-451. Режим доступа: http://www.bulletennauki.com/lavrushkina-a (дата обращения 15.04.2018).

Cite as (APA):

Lavrushkina, A. (2018). Typical investigations in the framework of the fraud investigation method with using the Internet network and mobile communication facilities. *Bulletin of Science and Practice,* 4, (4), 447-451