### К ВОПРОСУ О НЕКОТОРЫХ СПОСОБАХ СОВЕРШЕНИЯ "МОБИЛЬНЫХ" МОШЕННИЧЕСТВ

© 2020 Бикинеева Любовь Николаевна магистрант
© 2020 Хаснутдинов Ренат Рафаильевич кандидат юридических наук, доцент
Самарский государственный экономический университет E-mail: Khasnutdinoff@mail.ru

**Ключевые слова:** мошенничество, мобильная связь, SMS-сообщение, телефонный звонок, денежные средства.

В статье рассматриваются основные способы совершения мошенничеств с использованием средств мобильной связи, раскрываются алгоритмы действий преступников.

Научно-технический прогресс внес большие изменения в человеческую жизнь. За последние пятнадцать лет средства мобильной связи быстро эволюционировали и стали доступны всем гражданам нашей страны. Мобильные телефоны также значительно прогрессировали, и в настоящее время используются не только для совершения телефонных звонков и передачи SMS-сообщений, но и для перевода денежных средств и электронных платежей. В результате чего появились новые виды преступлений - хищения денежных средств путем дистанционного обмана либо злоупотребления доверием. Особенность таких преступлений заключается в том, что взаимодействие между преступником и потерпевшим происходит на расстоянии до нескольких тысяч километров, при помощи устройства - мобильного телефона. Наивность и доверчивость граждан приводит к тому, что преступники за кроткий промежуток времени получают от потерпевших крупные суммы денежных средств.

Согласно статистическим данным МВД России, большую часть (около 60%) от общего числа зарегистрированных мошенничеств общеуголовной направленности составляют мошенничества, совершенные с использованием средств мобильной связи<sup>1</sup>.

Преступник при помощи мобильного телефона может оказывать воздействие на потерпевшего посредством телефонного звонка либо SMS-сообщения. Основная цель - завладеть денежными средствами потерпевшего. Для этого используются различные способы.

## 1. Обман в ходе телефонного звонка.

На абонентский номер гражданина поступает телефонный звонок с незнакомого абонентского номера. В ходе разговора мошенник представляется знакомым или родственником абонента и сообщает о том, что он попал в беду, а именно его задержали сотрудники полиции за совершение преступления (дорожно-транспортного происшествия, где имела место смерть пассажиров, пешеходов или водителя; преступления, связанного с

незаконным оборотом наркотических средств и т.д.). После чего переедет трубку якобы сотруднику полиции, который разъясняет, что может помочь родственнику избежать ответственности за преступление, однако, для решения вопроса необходима определенная денежная сумма. Поясняет, что деньги нужны для урегулирования вопроса со свидетелями и потерпевшими. Денежные суммы варьируются от нескольких тысяч до нескольких миллионов рублей. Далее преступник объясняет, каким образом необходимо передать денежные средства (перевести на банковский счет, отправить почтовый перевод, передать лично другому человеку и т.д.). До передачи денежных средств мошенник ведет непрерывный телефонный разговор, для того, чтобы потерпевший не смог связаться со своим родственником, о котором идет речь, и распознать обман².

Другим способом телефонного обмана может стать звонок сотрудника банка. На мобильный телефон потерпевшего поступает звонок, в ходе разговора мошенник представляется сотрудником финансового учреждения и сообщается информацию о том, что с карты абонента совершена попытка несанкционированного снятия денежных средств, в результате чего в целях безопасности банковская карта была заблокирована. Чтобы войти в доверие, мошенник использует фразу: "Никому не сообщайте данные по картам, кроме сотрудников банка". После чего, выясняет у потерпевшего кодовую информацию по карте (номер карты, срок действия, код карты, расположенный на оборотной стороне), тем самым получает доступ к его денежным средствам. В настоящее время мошенники могут использовать абонентские номера банков (например, преступники могут позвонить с абонентского номера 900 и представиться сотрудниками ПАО "Сбербанк")3.

#### 2. SMS-сообщения с просьбой о помощи.

На абонентский номер гражданина поступает SMS-сообщение с текстом: "Мама, у меня проблемы, кинь 700 рублей на этот номер. Мне не звони, перезвоню сам". Мошенник набирает номер наугад, поэтому пишет текст с различным обращением "папа", "брат" и т.д., в надеже на доверчивость жертвы. Данная схема мошенничества наиболее проста, так как преступник не ведет с потерпевшим длительных переговоров. Такому способу мошенничества особо могут быть подвергнуты пожилые люди<sup>4</sup>.

### 3. Перевод денежных средств по ошибке.

Еще одной простой схемой "мобильного" мошенничества является - "перевод денежных средств по ошибке". На абонентский номер гражданина поступает SMS-сообщение, согласно которому на его счет зачислены денежные средства. Через некоторое время поступает новое SMS-сообщение или телефонный звонок, в ходе которого мошенник сообщает, что перевел денежные средства по ошибке и просит вернуть их обратно.

# 4. Абонентский номер-грабитель.

В настоящее время существует множество различных сервисов с платным звонком (например, развлекательные телевизионные шоу-программы). Владельцы указанных абонентских номеров обязаны информировать граждан о плате, взимаемой за звонок. Регистрируя такой сервис, мошенники используют его в своих преступных целях. Не информируют население о взимаемой плате.

На абонентский номер гражданина поступает SMS-сообщение с просьбой перезвонить на указанный абонентский номер. Просьба может быть обоснована любой причиной - помощь близкому родственнику, проблемы с банковской картой и др. При осуществлении

телефонного звонка, абонент длительное время ожидает ответа. На звонок никто не отвечает, а за ожидание списываются денежные средства.

5. Предложение о получении доступа к SMS-сообщениям и звонкам другого абонента.

Несомненно, многие граждане хотели бы иметь возможность следить за свои родственники, близкими или знакомыми, преследуя при этом различные цели. Зная это, мошенники разработали очередной способ получения денежных средств от граждан преступным путем.

Так, абоненту поступает SMS-сообщение с предложением о возможном доступе к входящим и исходящим телефонным звонкам и содержанию SMS-сообщений интересующего абонента. Для чего необходимо отправить SMS-сообщение на определенный номер, с указанием номера телефона интересующего абонента. В предложении указывается незначительная стоимость услуги (около 30 рублей). После того, как потерпевший отправляет SMS-сообщение с указанием интересующего его абонентского номера, с его счета списывается сумма в несколько раз больше той, что было заявлено в предложении (около 500 рублей), а обещанная информация так и не поступает<sup>4</sup>.

# 6. Несуществующие объявление.

На сегодняшний день покупка и продажа товаров, бывших в употреблении, получила широкое распространение благодаря таким площадкам как "Авито", "Юла" и др., которые мошенники также стали использовать в своих преступных целях. Большое количество мошенничеств связны с продажей подержанных автомобилей.

Так, гражданин, располагая определенной денежной суммой, принимает решение о покупке подержанного автомобиля, для чего обращается к указанным выше сайтам, где находит объявление о продаже хорошего автомобиля по низкой стоимости. В объявлении, как привило, указывается фраза: "Срочная продажа!" В надежде на выгодную сделку, абонент звонит якобы продавцу. Последний, в ходе телефонного разговора, сообщает свою печальную историю, например, о том, что ему срочно необходимы денежные средства на лечение его близкого родственника, в связи с чем, он готов расстаться со своим автомобилем, а цена такая низкая, так как деньги нужны срочно. После чего, сообщает, что в ближайшее время автомобиль осмотреть невозможно (машина в гараже, а ключи у родственника; автомобиль находится в другом населенном пункте; позднее время суток и т.д.), однако, денежные средства нужны прямо сейчас. Поэтому мошенник предлагает потерпевшему перевести (передать) определенную денежную сумму в качестве залога, в противном случае он продаст машину другим лицам. При этом мошенник, чтобы заинтересовать жертву утверждает, что автомобиль в хорошем состоянии, за такие деньги такой автомобиль купить более не представится возможным. В случае передачи денежных средств, объявление о продаже удаляется, а мошенник более не выходит на связь.

# 7. Подтверждение персональных данных.

В связи с изменениями ФЗ "О связи" 5, вступившими в силу 01 июня 2018 года, появился еще один способ "мобильного" мошенничества. Законодатель обязал операторов связи проверить достоверность сведений, которые были предоставлены их абонентами. К ним относятся: дата рождения, фамилия, имя, отчество, данные паспорта. Если данные абонента не будут совпадать с теми, которые уже внесены в государственную информационную базу, оператор приостановит оказание услуг. Если запрос поступит от правоохранительных органов и в течение 15 дней абонент не подтвердит свои данные, оператор заблокирует сим-карту.

Так, гражданину на абонентский номер поступает SMS-сообщение, якобы от оператора связи, с требованием подтверждения паспортных данных, посредством отправления сканированной копии документа на определенный адрес. В сообщении так же указывается, что если скан не поступит в течение ближайших 15 дней, номер будет заблокирован.

Большинство потерпевших, получивших указанное сообщение, обращаются к сети Интернет, где видят соответствующие изменения в законодательстве и отправляют копии паспортов по адресу, указанному в SMS-сообщении. Далее при помощи копии паспорта мошенники могут оформить на имя потерпевшего заем в микрофинансовой организации, заключить различного рода сделку и т.д.

В статье приведены далеко не все способы совершения "мобильных" мошенничеств, так как с каждым днем происходят различного рода изменения, в связи с чем, преступники создают новые схемы для обмана граждан. Тем не менее, правоохранительным органам необходимо постоянно мониторить новые способы совершения данных преступлений, поскольку от этого напрямую зависит качество, быстрота и полнота раскрытия и расследования уголовных дел по мошенничествам, совершенным с помощью мобильных устройств.

# TO THE QUESTION ABOUT SOME WAYS OF PERFORMING "MOBILE" FRAUD OF INSUITS

© 2020 Bikineeva lubov Nikolaevna Undergraduate © 2020 Khasnutdinov Renat Rafailevich Candidate of law, associate Professor Samara State University of Economics E-mail: Khasnutdinoff@mail.ru

Keywords: fraud, mobile communications, SMS, phone call, cash.

The article discusses the main ways of committing fraud using mobile communications, reveals the algorithms of the criminals.

¹. Состояние преступности в России за январь-декабрь 2019 // МВД РФ ФКУ "Главный информационно-аналитический центр".

<sup>&</sup>lt;sup>2.</sup> Материалы уголовного дела по обвинению Г. 2017 г. // Архив Промышленного районноо суда г. Самары.

 $<sup>^{3.}</sup>$  Материалы уголовного дела по обвинению Г. 2019 г. // Архив Железнодорожного районноо суда г. Самары.

<sup>&</sup>lt;sup>4</sup> Лабутин А.А. "Мобильные" мошенничества: основные способы совершения // Вестник Казанского юридического института МВД России. 2013. № 2(12). С. 50-55.

<sup>&</sup>lt;sup>5.</sup> Федеральный закон РФ "О связи" от 7 июля 2003 г. N 126-ФЗ (с изм.) [Эл. ресурс] // СПС "КонсультантПлюс"(дата обращения 29.02.2020).