ЮРИСПРУДЕНЦИЯ

Михалёв Андрей Владимирович
старший преподаватель
Новороссийский филиал Краснодарского университета МВД России
г. Новороссийск, Краснодарский край

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ТЕЛЕФОННЫХ МОШЕННИЧЕСТВ С БАНКОВСКИМИ КАРТАМИ НА ПЕРВОНАЧАЛЬНОМ ЭТАПЕ

Аннотация: *в статье затрагиваются проблемы в сфере оборота пластиковых карт, автором рассмотрен опыт проведения первоначальных следственных действий при получении сообщения о телефонных мошенничествах, связанных с банковскими картами.*

Ключевые слова: *банковские карты, преступники, злоумышленники, телефонные мошенничества, первоначальные следственные действия.*

Все больше людей и в нашей стране пользуются банковскими картами. Многие имеют по несколько карт [1]. Банковские карты во многом облегчают повседневные расчеты, позволяют отказаться от хранения наличных денежных средств и имеют много других преимуществ. Большинство людей считают это средство расчетов удобным, надежным, практичным. Вместе с тем, Российская Федерация переживает достаточно сложный период становления новых социально-экономических отношений. Имеются дефицит и противоречия в правовой базе, регулирующей экономические отношения.

На протяжении последних лет наблюдается устойчивый рост преступлений в сфере экономических отношений, в том числе и сфере оборота пластиковых карт. К сожалению, далеко не все пострадавшие обращаются в правоохранительные органы, или обращаются не вовремя, спустя продолжительное время после совершения преступления, а те обращения, которые все-таки регистрируются в органах внутренних дел, чаще всего попадают в категорию так называемых «не

раскрываемых дел». Преступники технически грамотны, обладают неординарным мышлением, пользуются доверчивостью и неграмотностью в правовых и экономических вопросах пострадавших.

В настоящей статье будет рассмотрен опыт проведения первоначальных следственных действий при получении сообщения о телефонных мошенничествах, связанных с банковскими картами.

Сотрудники Управления Министерства внутренних дел РФ по Кировской области задержали группу мошенников, снявших с банковских счетов жителей Российской Федерации в разных регионах более 50 миллионов рублей [2]. В группировку входили пять человек. Это жители Кировской области, Пермского края и Республики Коми. По данным фактам было возбуждено более 20 уголовных дел по статье 159 Уголовного кодекса РФ [3] (мошенничество). Это цифра не окончательная, поскольку, по оперативным данным, было не менее 50 мошеннических транзакций. Жертвами преступления стали жители Кировской и Московской областей, города Санкт-Петербурга, Республики Татарстан и Краснодарского края.

В ходе следствия сотрудниками полиции было установлено, что злоумышленниками осуществлялась «веерная» рассылка сообщений СМС держателям банковских карт MasterCard и Visa, с уведомлением о том, что их карта заблокирована. В сообщении они указывали номер телефона для справок, внешне сходный с бесплатным справочным телефонным номером банка. Это был обычный абонентский номер города Москвы, с которого шла переадресация на мобильный телефон мошенников. Получив сообщение, человек, ничего не подозревая, в панике начинал звонить по указанному номеру. Путем наводящих вопросов, якобы требующихся для того, чтобы «удостоверить личность» звонившего, мошенники в течение нескольких минут получали всю необходимую информацию – от личных данных владельца карты до данных карты: номера, даты выдачи и CVS кода.

Пользуясь доверчивостью потерпевших и выдавая себя за сотрудников банков, злоумышленники уверенно объясняли владельцам карт причину ее блоки-

ровки, а именно, что с помощью специального устройства (скиммера) неизвестные скопировали карту и пытались подобрать к ней пин-код, в связи с тем, что он три раза был введен неверно, карта была заблокирована. Далее мошенники сообщали, что для разблокировки карты на телефон жертвы из банка будет направлено СМС сообщение с одноразовым цифровым паролем, который жертва должна будет сообщить, перезвонив по вышеуказанному номеру. После этого, преступники с использованием компьютерных средств при помощи Internet-сервиса отдавали указание о совершении перевода денег со счета банковской карты жертвы на созданный ими виртуальный кошелек «Яндекс-деньги». Таким образом, используя данную преступную схему, злоумышленники только с карты одного из жителей Московский области за одну транзакцию похитили более 500 тысяч рублей. Общая сумма нанесенного ущерба была оценена на сумму более 50 миллионов рублей.

Как мы видим, для совершения преступления достаточно знания реквизитов банковской карты и CVS кода. В некоторых банках, как например, в ОАО «Сбербанк России», для проведения операции также необходим одноразовый цифровой пароль. В ряде банков (например, Абсолют банк) наличие CVS кода является достаточным для проведения операции перевода денежных средств [4].

Существующие в настоящее время как технические, так и правовые недостатки защиты банковских карт создают предпосылки для сложности раскрытия указанных преступлений. Осложняет расследование преступления и то обстоятельство, что злоумышленников никто не видел, все общение происходит по телефону, они с конспиративной целью активно передвигаются не только в пределах одного города, но и в пределах страны.

На основании вышеизложенного, сотрудникам полиции необходимо проводить следующий *перечень первоначальных мероприятий*:

1. При получении сообщения о совершении данного вида преступления, прежде всего, необходимо правильно и грамотно допросить потерпевшего. При допросе особое внимание следует уделить фонетическим и лингвистическим признакам речи преступника (характеристики голоса по высоте, силе, тембру,

общем уровне образования и степени культуры, наличии дефектов речи (шепелявость, гнусавость, парез-затруднение в артикуляции произнесении отдельных звуков), наличие территориального диалекта (лексический запас слов, фраз, склонения, спряжения слов, фонетический строй, интонация, ударение, темп речи, наличие либо отсутствие акцента), наличие профессионализмов и жаргонизмов в речи). Данные признаки позволят определить примерный облик человека по признакам устной речи.

2. Провести осмотр телефона в качестве предмета, сфотографировать поступившие СМС сообщения и приложить их в виде фототаблицы к протоколу осмотра предмета (телефона), чтобы использовать в дальнейшем в качестве доказательств.

3. Особенностью данного вида преступлений является то, что мошенники после рассылки СМС сообщений в течении 1-2 суток находятся на одном телефонном номере и принимают все входящие звонки, поэтому необходимо произвести телефонный звонок по указанному в «веерной» рассылке абоненскому телефонному номеру и зафиксировать (записать при помощи технических средств) содержание телефонного разговора в целях лингво-акустического анализа речи мошенников, а также сопутствующей звуковой информации, по которой можно установить некоторые особенности окружающей обстановки. В дальнейшем мошенники избавляются от телефонного номера, выбросив сим-карту.

4. Сотрудникам оперативных подразделений необходимо помочь составить потерпевшему правильный с технической стороны запрос в центр - процессинг банка с просьбой приостановить следующие транзакции, так как они несанкционированные и приложить выписку. Как только транзакции приостановят, мошенники не смогут вывести деньги.

5. Также должны быть направлены запросы в сервисы банков с целью выяснения движения средств. Денежные средства некоторое время «висят», банки имеют право выдать справки о движении банковских средств и о вкладчиках.

Необходимо установить, куда направлены денежные средства, телефоны, IP адреса преступников. Для этого необходимо наиболее полно провести оперативную разработку преступников.

6. При разработке необходимо использовать детализацию телефонных разговоров, установить наиболее часто используемые базовые станции и, при помощи биллинга, определить примерное место нахождения преступника. Зная IP адрес выхода в сеть Internet, можно установить точный адрес нахождения преступников.

7. При проведении обысков необходимо изымать все телефонные аппараты, средства для выхода в Internet, системные блоки, ноутбуки, с целью проведения в дальнейшем компьютерной экспертизы. Необходимо также иметь ввиду, что преступники могут выдать себя тем, что долго используют одни и те же телефонные аппараты, что может быть распознано по регистрации imei телефона в сотовых сетях.

Список литературы

1. М.В. Хворостяный «Преступления, совершаемые с использованием банковских карт» http://www.pravoznavec.com.ua/period/article/4628/%CC.

2. Российская газета от 09.01.13 http://www.rg.ru/2013/01/09/reg-pfo/kirov-kart-anons.html.

3. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. Собрание законодательства РФ, 17.06.1996, № 25, ст. 2954.

4. «Положение о правилах осуществления перевода денежных средств» (утв. Банком России 19.06.2012 N 383-П) (ред. от 29.04.2014) 2Вестник Банка России», N 34, 28.06.2012.