УДК 343.9

С.Ю. Шушков*

СПОСОБЫ ПОЛУЧЕНИЯ ИНФОРМАЦИИ О БАНКОВСКИХ КАРТАХ ПРИ СОВЕРШЕНИИ МОШЕННИЧЕСТВА С ИХ ИСПОЛЬЗОВАНИЕМ

В статье анализируются способы получения информации о банковских картах, в целях последующего совершения мошенничества с использованием банковских карт.

Ключевые слова: пластиковая карта, мошенничество с использованием банковских карт, противоправный способ получения информации.

В настоящее время в мире насчитывается свыше миллиарда банковских карточек. Банковская карта (BC, BCard, Bank Card) – пластиковая карта, привязанная к одному или нескольким расчётным счетам в банке. Используется для оплаты товаров и услуг, в том числе через Интернет, а также снятия наличных. Карты бывают дебето́вые и кредитные. Дебето́вые карты используются для распоряжения собственными деньгами, находящимися на расчетном счете в банке. Кредитные карты используются для распоряжения деньгами банка, которые при совершении платежа автоматически берутся у банка в кредит (их требуется вернуть банку) [4, с. 5]. Как финансовый инструмент карточки постоянно совершенствуются, растет сфера их применения, расширяется поле оказываемых услуг по их использованию. Однако банковские пластиковые карточки, как всякий высокодоходный бизнес (особенно в сфере денежного обращения), давно стали мишенью для противоправных посягательств.

По данным статистики, в 2013 году в России количество банковских карт, эмитированных кредитными организациями составило 834 156 тысяч единиц, что на 15,3 % больше чем в 2012 г. [7]. Исходя из этого, можно сделать вывод, что платежные системы в Российской Федерации имеют весомое значение и их приоритет перед другими способами оплаты различного рода товаров вполне очевиден и оправдан. [1, с. 11]

Банковская карточка физически представляет собой пластину стандартных размеров (чаще всего ISO 7810 54 х 86 х 0.76 мм), изготовленную из специальной, устойчивой к механическим и термическим воздействиям пластмассы. Персонализация – процедура нанесения на платежную карту и (или) запись в память микропроцессора, на магнитную полосу платежной карты информации, предусмотренной кредитной организацией-эмитентом [6]. Информация находящаяся на карте и является основной целью мошенников, так как при помощи этой информации преступники получают доступ к счету.

Способы мошенничества с банковскими картами самые разнообразные. Наибольшую трудность для мошенников составляет получение данных о реквизитах карты и ПИН кода владельца. Сбор информации о кредитной карте

* Шушков Станислав Юрьевич – магистрант, кафедра криминалистики и судебных экспертиз, Байкальский государственный университет экономики и права, г. Иркутск, magistr@mail.ru.

может быть осуществлен путем использования интернета, кражи данных с компьютеров владельцев, с использованием специальных вирусов, взлома баз данных банков, торговых предприятий, сбора информации о кредитной карте без использования интернета, через банкоматы, кражи карты после совершения покупок в магазинах.

Последующее использование данных информации карты возможно для изготовления копий магнитной полосы карты и нанесения ее на кусок пластика, аналогичный по размеру с настоящей картой. Копия карты используется при снятии денег в банкомате, покупок через интернет, покупок в магазинах по безналичному расчету.

Получение ПИН кода является самым трудоемким процессом для мошенников. Получить эти данные можно несколькими способами:

1) Оглашение сведений о ПИН-коде самим держателем карты. Имеется ввиду, к примеру, запись ПИН-кода на карте или каком-либо носителе (лист бумаги, записная книжка, мобильный телефон), хранимом вместе с картой. Соответственно, если карта утеряна или украдена (вместе с сумкой, бумажником), у мошенника оказывается и карта и персональный код [2].

2) Дружественное мошенничество. Использование в своих целях карты с предварительной осведомленностью о ПИН-коде членами семьи, близкими друзьями, коллегами по работе. То есть людьми, имеющими доступ к месту хранения карты [2].

3) Подглядывание из-за плеча. Мошенник вполне может узнать ПИН-код держателя банковской карты, подглядывая из-за его плеча, фиксировать с помощью средств видео фиксации, пока тот вводит код в банкомате. Затем злоумышленник осуществляет кражу карты и использует ее в своих целях [2].

4) «Ливанская петля». Целью ее использования является хищение карты держателя и компрометация ее ПИН-кода. С этой целью преступники используют специальные механические приспособления, под воздействием которых карта застревает в картридере(отверстие банкомата, в которое вставляется карта). Зачастую таким устройством служит устанавливаемая на подлинный картридер дополнительная накладка. Как только клиент замечает, что карта оказалась якобы захваченной банкоматом (на самом же деле она остается в накладном устройстве картридера), на сцене появляется мошенник, который либо заранее уже подсмотрел введенный ПИН-код, либо предлагает свою помощь с целью получения данных ПИН-кода. Мошенник доходчиво и красочно рассказывает легенду о том, что если клиент введет ПИН-код повторно, то транзакция продолжится, чего, естественно, в итоге не происходит. Как только ничего не подозревающий клиент отходит от банкомата с намерением обратиться в службу поддержки банка, мошенник извлекает карту из ранее установленного приспособления. Имея в своем распоряжении карту и зная ПИН-код, мошенник без проблем тут же снимает деньги со счета законного держателя карты [3].

5) Фальшивые банкоматы – достаточно редкий способ, требующий технической оснащённости. Мошенники изготавливают фальшивые банкоматы, которые выглядят как настоящие, либо переделывают старые, и размещают их в людных местах. Такой банкомат принимает карту, требует ввода ПИН-кода,

после чего выдаёт сообщение о невозможности выдачи денег (под предлогом отсутствия денег в банкомате или технической ошибки) и возвращает карту. В банкомате происходит копирование данных карты, а также фиксация камерой вводимого ПИН-кода, что позволяет мошенникам впоследствии изготовить дубликат и снять с его помощью деньги со счета клиента [3].

6) Скимминг – (от англ. to skim – снимать сливки) мошенничество, при котором используется скиммер – инструмент злоумышленника для считывания данных магнитной полосы банковской карты. При осуществлении данной мошеннической операции используется комплекс скимминговых устройств, таких как:

– устройство, устанавливаемое в картридер. Скимменговые устройства могут быть портативными, миниатюрными. Основная идея и задача скимминга – считать необходимые данные с магнитной полосы карты для последующего их воспроизведения на поддельной карте (т.н. «белый пластик»). В итоге, при осуществлении мошенниками операции по поддельной карте, списание денежных средств будет осуществлены со счета оригинальной, «скиммированной» карты.

– Специальная накладка на клавиатуру банкомата, либо миниатюрная видеокамера, устанавливаемая на банкомат и направляемая на клавиатуру. Данные устройства используется вкупе со скиммером для получения ПИН-кода держателя, что позволяет получать наличные в банкоматах по поддельной карте (имея данные магнитной полосы и ПИН-кода оригинальной карты). Данные устройства, как правило, изготавливаются и маскируются под цвет и форму банкомата [3].

7) Шимминг представляет собой разновидность скимминга. Тогда как последний характеризуется накладками на банкоматы, которые можно при желании увидеть и прощупать, шимминг абсолютно не заметен. Шиммер – электронное устройство (тонкая гибкая плата), которое тоньше человеческого волоса (толщина составляет примерно 0,2 мм), абсолютно не заметно держателю карты. Шиммер помещается через щель картридера и считывает данные введенных карт [3].

8) Фишинг (от англ. fishing – рыбная ловля, выуживание) – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным владельца Карты. Это достигается путем проведения рассылок sms-сообщений/ электронных писем, от имени популярных брендов, внутри различных сервисов или социальных сетей, а также от имени Банка. Мошенники пытаются различными психологическими приёмами побудить клиента отослать свои персональные данные, а также реквизиты своей карты. Помимо этого, в письме часто содержится прямая ссылка на сайт «Банка», внешне не отличимый от настоящего. Мошенники часто пытаются сделать так, чтобы клиент попадал на поддельную страницу сайта, на которой бы он вводил все необходимые злоумышленникам данные [3].

9) Вишинг (от англ. vishing – voice phishing) назван так по аналогии с фишингом. Сходство названий подчеркивает тот факт, что принципиальной разницы между вишингом и фишингом нет. Основное отличие вишинга в том, что

так или иначе задействуется телефон. Целью вишинга, так же, является получение доступа к конфиденциальным данным владельца Карты [3].

10) Миниатюрная видеокамера. Может быть замаскирована под коробку для раздачи рекламных листовок и визиток. Коробка ставится сверху на банкомат, либо подвешивается в непосредственной близости у клавиатуры банкомата [2].

11) Неэлектронный фишинг. Данный вид связан с осуществлением покупок в торговых организациях посредством обязательного ввода ПИН-кода. В схемах неэлектронного фишинга создаются реальные торгово-сервисные предприятия/офисы банков, либо используются уже существующие. Держатели платежных карт совершают покупки товаров, получают услуги либо снимают денежные средства в кассе банка. Операции производятся с использованием банковских микропроцессорных карт и сопровождаются введением клиентом своего ПИН-кода. Сотрудники мошеннических предприятий негласно копируют информацию с магнитной полосы карты и производят запись персонального идентификационного номера. Далее мошенники изготавливают поддельную банковскую карту, и в банкоматах производится снятие денежных средств со счета клиента [2].

12) Вирус, поражающий банкоматы. Новейшим изысканием мошенников стал вирус, который отслеживает производимые операции и ворует информацию с пластиковых карт, передавая ее мошенникам. По данным портала Рубль.ру способ, выбранный злоумышленниками весьма замысловат. Написать вредоносную программу для банкомата очень сложно – мошенники используют очень специфические операционные системы и связываются с банками по серьезно защищенным сетям [2].

Сотрудники правоохранительных органов (следователи, сотрудники оперативных подразделений) на практике сталкиваются с серьезными трудностями при расследовании преступлений, совершенных при помощи банковских карт и их реквизитов. Расследование уголовных дел по мошенничеству с использованием банковских карт предполагает наличие более обширных знаний как в области криминалистики (вопросы изготовления, эксплуатации и защиты банковских карт, принципы функционирования платежных систем), так и в сфере уголовно-правовой регламентации (мониторинг международное и российское законодательство по рассматриваемой тематике). Это объясняется прежде всего, особыми свойствами предмета правонарушения – банковской карты.

Основным признаком мошенничества с использованием банковских карт, выделяющим его из остальных многочисленных видом мошенничества, является сама банковская карта, как средство совершения преступления. Исходные данные неразрывно связаны с исходными сведениями о банковской карте и характерными данными о месте и времени совершения преступления, об используемых при совершении преступления производственных, финансовых либо учетных операциях, о способах хищения, субъектах.

В заключение обратим внимание на то, что успешное внедрение в сферу розничных платежей систему расчетов с использованием платежных карт во многом зависит от того, насколько защищены права их держателей, так как за последние годы преступность в сфере использования банковских карт очень

сильно возросла. Ущерб от хищений, совершаемых с использованием банковских карт и их реквизитов, с каждым годом увеличивался и составил в 2011 г. свыше 2,68 млрд р., что почти в два раза больше, чем в 2010 [5].

Мошенничество с банковскими картами развивается вместе с развитием банковских технологий. Внедрение банковских карт и использование компьютерных технологий в сфере платежей покупок, кредитования являются характерной чертой повседневной жизни. Изучение способов мошенничества с банковскими картами в первую очередь необходимо для разработки средств и методов защиты от данного вида преступления, а так же успешного выявления и изобличения лиц совершивших мошенничество с использованием банковских карт.

Список использованной литературы

1). Алексанов А.К., Доронин А.М., Демчев И.А. и др. Безопасность карточного бизнеса. Бизнес-энциклопедия. – МФПА: ЦИПСиР 2011. – 277с.

2) Мошенничество с банковскими картами // официальный сайт biz-incom.ru [Электронный ресурс] http://biz-incom.ru/moshennichestvo-s-bankovskimi-kartami (дата обращения: 06.05.2014).

3) Официальный сайт банка «Кубань Кредит» [Электронный ресурс] // http://www.kubankredit.ru/fizicheskim/bankovskie. (дата обращения: 06.05.2014).

4) Порядок №299-2-р – «Порядок совершения операций с международными банковскими картами в подразделениях Сбербанка России (Эмиссия)» от 16 мая 2002 г. №299-2-р // СПС «Гарант»

5) Филиппов М. Н. Расследование краж и мошенничеств, совершенных с использованием банковских карт и их реквизитов: автореф. дис. канд. юрид. наук (12.00.09) М., 2012 [Электронный ресурс] // http://www.rg.ru/2011/11/03/karty.html (дата обращения: 06.05.2014).

6) Положение об эмиссии платежных карт и об операциях совершаемых с их использование : Приказ Центрального банка Российской Федерации 24 декабря 2004 г. № 266-п // СПС «Консультант Плюс»

7) Количество расчетных и кредитных карт, эмитированных кредитными организациями : официальный сайт ЦБ РФ [Электронный ресурс] http://www.cbr.ru/statistics/p_sys/print.aspx?file=sheet007.htm (дата обращения: 06.05.2014).