УДК 336.74

Фурманов Дмитрий Витальевич, Смольянинова Елена Николаевна

Владивостокский государственный университет экономики и сервиса
Владивосток, Россия

Усугубление проблемы безопасности при использовании пластиковых карт

Одной из актуальных проблем банковской системы является вопрос о безопасности хранения денежных средств на счетах клиентов банка, в том числе и в масштабах нашей страны, поскольку с каждым годом число мошеннических операций имеет положительный тренд, а суммы теряемые клиентом принимают значительные размеры. В рамках данной статьи рассматриваются основные способы мошенничества с пластиковыми картами и возможные способы защиты от мошенничества.

Ключевые слова и словосочетания: *Банки, пластиковые карты, мошенничество, скримминг, фишинг.*

Коммерческие банки, как и другие субъекты хозяйственных отношений, для обеспечения своей коммерческой и хозяйственной деятельности должны располагать определенной суммой денежных средств, то есть ресурсами. В современных условиях развития экономики проблема формирования ресурсов имеет первостепенное значение. «От правильного выбора пассивов, точного определения стратегии и тактики управления ими зависит получение положительного финансового результата банка» [1, С. 140].

Масштабы деятельности банка, определяемые объектом его активных операций, зависят от совокупной суммы ресурсов, которыми он располагает, особенно от суммы привлеченных ресурсов. Такое положение обостряет конкурентную борьбу между банками за привлечение ресурсов.

Исследование, проведенное агентством ProfiOnlineResearch, выявило высокий уровень вовлеченности россиян в сферу банковских услуг. «В целом, клиенты банков достаточно высоко оценивают предоставляемый уровень обслуживания». Анализ данных показал, что более 50% респондентов использовали зарплатные карты, а следующим по популярности видом услуг является вклад (вне зависимости от условий привлечения). Пользуются теми или иными видами вкладов около 33% участников исследования. А на третьем месте по популярности среди опрашиваемых расположились кредитные и дебетовые карты. На текущий момент такие

банковские услуги, как ипотека, инвестиции, кредиты на образование, аренда банковской ячейки и др., мало востребованы среди россиян: к ним прибегают не более 6% респондентов [2].

Таким образом, можно сделать вывод, что в настоящий момент среди физических лиц наиболее распространёнными являются операции по зарплатным картам и вкладам.

В рамках данного исследования и на основании вышеизложенного хотелось бы обратить внимание на проблему мошенничества с пластиковыми картами, т.к. ежегодно оборот по банковским картам растет в нашей стране и на конец 2011 года, по данным экспертов, оборот по пластиковым картам будет превышать 13 трлн руб.

Физические лица, используя пластиковые карты в расчетах, начинают носить в кошельке меньше наличных денег, все больше и больше доверяя пластику, но в связи с тем, что деньги стали электронными и мошенники, заполучив кошельки жертв, видят там только куски пластика вместо наличных, злоумышленники начали придумывать различные способы заполучить средства своих жертв.

По мнению управления ЦБ РФ: «К концу 2011 года ущерб от мошенничества с кредитными картами ожидается в размере 2,68 млрд рублей, что почти в два раза больше, чем в прошлом году…» [3], следовательно, количество мошеннических операций с каждым годом растёт.

С развитием Интернета и появлением «виртуальных магазинов» стало возможным заказывать товары по почте с персонального компьютера, в связи с этим поле для махинаций с пластиковыми карточками значительно расширилось. Для оплаты заказанного товара достаточно указать реквизиты карточки, следовательно, любая информация о карточке для владельца может обернуться невосполнимыми потерями. А способов выманивания реквизитов карточек у владельцев – великое множество. Растущий вал преступлений в этой сфере, по мнению некоторых специалистов, грозит подорвать авторитет карточек как надежного финансового инструмента, чтобы это предотвратить, рекомендуется предпринять следующие меры:

- увеличить число степеней защиты пластиковых карточек;
- обезопасить микропроцессоры от нежелательных атак извне;
- хранить пластиковые карточки в надежных местах и подальше от посторонних глаз;
- незамедлительно блокировать счета в банке в случае утраты пластиковой карточки;
- защитить компьютерные сети от взломщиков.

Рассмотрим наиболее распространенные схемы мошенничества с банковскими картами [4]:

1) Оглашение сведений о ПИН-коде самим держателем карты, к примеру, запись ПИН-кода на карте или каком-либо носителе, хранимом вместе с картой.

2) Дружественное мошенничество, т.е. использование в своих целях карты с предварительной осведомленностью о ПИН-коде членами семьи, близкими друзьями, коллегами по работе.

3) Подглядывание из-за плеча. В этом случае мошенник может узнать ПИН-код держателя банковской карты, подглядывая из-за его плеча, пока тот вводит код в банкомате, и осуществить кражу карты.

4) «Ливанская петля». Как вариант подглядывания из-за плеча. Пока владелец карточки погружает ее в банкомат, она застревает. В это время подходит «советчик», который рекомендует срочно идти и звонить в сервисную службу банка, а сам тем временем вытаскивает карту и снимает деньги.

5) Фальшивые банкоматы. Мошенники разрабатывают и производят фальшивые банкоматы либо переделывают старые, которые выглядят как настоящие. После введения карты и ПИН-кода обычно на дисплее фальшивого банкомата появляется надпись, что денег в банкомате нет или что банкомат не исправен. К тому времени мошенники уже скопировали с магнитной полосы карты информацию о счете данного лица и его персональный идентификационный номер.

6) Скримминг, смысл которого заключается в том, что при помощи нехитрых технических устройств делается копия пластиковой карты, узнаётся ПИН-код и спокойно обналичивается в банкомате дубликат.

7) Ложный ПИН-ПАД, когда держателю карты предлагают ввести ПИН-код в имитацию ПИН-ПАДА (ложные устройства), которая запомнит введенный код.

8) Ограбление держателей банковских карт.

9) Фишинг (fishing – рыбалка) – вид мошенничества в Интернете, который основывается на том, что злоумышленники «выуживают» у жертвы реквизиты его карты.

10) Вишинг (англ. vishing) – новый вид мошенничества, есть еще голосовой фишинг, использующий технологию, позволяющую автоматически собирать информацию, такую, как номера карт и счетов.

11) Неэлектронный фишинг. Данный вид связан с осуществлением покупок в торговых организациях посредством обязательного ввода ПИН-кода.

Проблеме борьбы с мошенничеством с пластиковыми картами уделяется большое внимание не только правоохранительными организациями [5; 6, Ст. 159], но и банковскими системами и сообществами разных стран [7 – 9]. Для Российской Федерации данная проблема также стоит доволь-

но остро, регулярно проводятся семинары, обучения, консультации и прочие мероприятия среди банкиров, в ходе которых раскрываются проблемы безопасности, механизмы защиты пластиковых карт, защита банкоматов, а также методы борьбы с мошенничеством и расследование преступлений [10 – 12].

На сегодняшний день не существует однозначного ответа на вопрос: «Как обезопасить себя от мошенничества с пластиковой картой?». Как правило, все советы сводятся к следующему: соблюдать нехитрые правила безопасности, которые, на наш взгляд, можно условно разделить на три группы:

1. Принцип «НЕ»: Не доверять карты третьим лицам, не оставлять их без присмотра, не записывать ПИН-код в легкодоступных местах и тем более на самой карте, НЕ сообщать свой ПИН-код, его не вправе требовать ни работники банка, выдавшего карту, ни обслуживающий персонал банкомата, не упускайте карту из виду, расплачиваясь в ресторанах или магазинах и т.д.
2. Принцип «ПРОВЕРЯЙ». Проверяй движения денег на карточном счете, проверяй операции по счету, проверяй, все ли было взято из банкомата и т.д.
3. «СООБЩАЙ». Сообщай в банк о потере или краже платежной карты, сообщай при появлении малейших подозрений о неправомерном списании денег со счета и пр.

Некоторые «продвинутые» банки уже предоставляют услугу страхования пластиковых карт от утери и связанных с ней рисков мошенничества. Правда, по словам банковских работников, клиенты не спешат пользоваться такой услугой. Причина этому проста: цена эмиссии новой карты при утере старой не на много выше платы за страховку. Поэтому многие клиенты не хотят тратить лишние деньги на страховку. А ведь она в случае мошенничества с картой обеспечила бы владельцам полное возмещение всех украденных средств [13].

На круглом столе, проводимом ЦБ РФ на тему: «Пресечение и профилактика мошенничеств с банковскими картами», начальник управления развития розничных платежей департамента регулирования расчетов Банка России Вадим Кузнецов обратил внимание на принятый недавно закон о национальной платежной системе. Многие его нормы как раз посвящены клиентам, осуществляющим перевод денежных средств с помощью карт, и, в частности, если произошло несанкционированное списание средств, банк обязан их возместить [3]. Тем не менее, по результатам встречи эксперты подчеркнули, что главным способом избежать мошенничества по-прежнему остается внимательность владельца банковской карты [3].

Таким образом, становится очевидным, что все проблемы, возникающие при использовании пластиковых карт, полностью возлагаются на клиентов.

---

1. Фисенко А.И., Смольянинова Е.Н. Маркетинговые программы депозитных операций в коммерческих банках: монография. – Владивосток: Дальнаука, 2007. – 276 с.

2. Опрос: В какой банк обратиться? [Электронный ресурс]. Доступно на URL: http://bankir.ru/novosti/s/opros-v-kakoi-bank-obratitsya-2179477/#ixzz1U6pHPZpT.

3. ЦБ РФ: ущерб от мошенничества с пластиковыми картами в 2011 году вырастет почти вдвое, до 2,68 млрд рублей [Электронный ресурс]. Доступно на URL: http://www.banki.ru/news/lenta/?id=3354208.

4. Александр Захаров Мошенничества с пластиковыми картами и их подделка [Электронный ресурс]. Доступно на URL: http://www.aferizm.ru/poddelka/valuta/ pp_plast_kart.htm.

5. Официальный сайт Управления прав потребителей. Отдел арбитражного контроля сети Интернет [Электронный ресурс]. Доступно на URL: http://www.webtrust.ru/no_trust/documents19.php.

6. Уголовный кодекс РФ (УК РФ) от 13.06.1996 № 63-ФЗ.

7. Мошенничество в Интернете [Электронный ресурс]. Доступно на URL: http://www.infousa.ru/information/internet_fraud.htm.

8. Internet Fraud Initiative Continues To Expand As A Global Medium [Электронный ресурс]. Доступно на URL: http://www.investmentfraudlawfirms. com/regional-content.cfm/state/tx/Article/12256/Internet-Fraud-Initiative-Continues .html.

9. Internet Crime Complaint Center [Электронный ресурс]. Доступно на URL: http://www.ic3.gov/default.aspx.

10. Механизмы защиты пластиковых карт от мошенничества, банкоматное мошенничество и расследование преступлений [Электронный ресурс]. Доступно на URL: http://bankir.ru/obuchenie/s/mekhanizmy-zashchity-plastikovykh-kart-ot-moshennichestva-bankomatnoe-moshennichestvo-i-rassledovanie-prestuplenii-571/#ixzz1myiWUQiV.

11. Проблемы безопасности и особенности защиты пластиковых карт от мошенничества. Банкоматное мошенничество. Преступления в сфере ДБО [Электронный ресурс]. Доступно на URL: http://bankir.ru/obuchenie/s/problemy-bezopasnosti-i-osobennosti-zashchity-plastikovykh-

kart-ot-moshennichestva-bankomatnoe-moshennichestvo-prestupleniya-v-sfere-dbo-795/#ixzz1myihFEfF.

12. Илья Сачков «Через два года хакеры будут лоббировать свои законы» [Электронный ресурс]. Доступно на URL: http://bankir.ru/ publikacii /s/ilya-sachkov-cherez-dva-goda-khakery-budut-lobbirovat-svoi-zakony-10001103/#ixzz1myjUacmN.

13. Энциклопедия мошенничества [Электронный ресурс]. Доступно на URL: http://www.gorodfinansov.ru/wallet/lfpiramid.php?ELEMENT_ID=5927.