МОШЕННИЧЕСКИЕ ОПЕРАЦИИ С БАНКОВСКИМИ ПЛАСТИКОВЫМИ КАРТАМИ КАК УГРОЗА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ В СФЕРЕ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ

УДК 336.71, 343.72

Елена Владимировна Илинич,
к.э.н., старший преподаватель кафедры финансов и экономического анализа Московского университета МВД России
Тел.: 8 (926) 285-85-57
Эл. почта: elena-ilinich@yandex.ru

Активное развитие банками безналичных расчетов пластиковыми картами, рост количества мошеннических операций и наносимого ими ущерба, создают новые вызовы и угрозы экономической безопасности в сфере банковской деятельности. Новейшие информационные технологии активно используют организованные преступные группировки, меняются способы совершения преступлений, которые пока не находят адекватного отражения со стороны банков и правоохранительных органов.

Ключевые слова: коммерческие банки, платежная система, банковские пластиковые карты, преступления, мошенничество, правоохранительные органы

Elena V. Ilinich,
PhD, Senior Lecturer, the Department of finance and the economic analysis, the Moscow University of the MIA of Russia
Tel.: 8 (926) 285-85-57
E-mail: elena-ilinich@yandex.ru

FRAUDULENT TRANSACTIONS WITH BANK PLASTIC CARDS AS A THREAT TO ECONOMIC SECURITY IN THE BANKING SPHERE.

Banks active development of cashless payments by plastic cards, the growing number of fraudulent transactions and the damage they cause, create new challenges and threats to economic security in the sphere of banking activity. The latest information technologies are active used by organized crime groups, the methods of committing crimes are changing and are not yet adequately reflected by banks and law enforcement agencies.

Keywords: commercial banks, payment system, plastic cards, crime cases, fraud, law enforcement officer.

1. Введение

На сегодняшний день правонарушения в сфере банковской деятельности представляют серьезную угрозу экономическим интересам всего общества. В результате интенсивного развития и внедрения современных информационных технологий в мире активизировались процессы формирования глобального информационного пространства, повлекшие за собой и появление новых вызовов и угроз.

Современные платежные системы предоставляют организованной преступности широкие возможности по отмыванию денежных средств, полученных преступным путем, финансированию терроризма, выводу капитала за рубеж, что связано, прежде всего, с возможностью использования большого числа финансовых инструментов и современных информационных технологий, а также обезличенностью денег, находящихся в обращении.

Ежедневно в мире около 2 трлн. долларов перечисляются с использованием электронных систем. При этом банки и другие финансовые посредники пытаются расширить свою деятельность в интернете, чтобы, в первую очередь, значительно уменьшить свои административные затраты, а также дать возможность своим клиентам более эффективно управлять своими счетами. Кроме того, многие компании из-за жесткой конкуренции вынуждены проводить большую часть своих бизнес-коммуникаций в интернете, что без должного отношения к вопросам защиты информации делает их более уязвимыми для преступников.

По данным Computer Emergency Response Team (CERT), международного авторитета в области безопасности Интернета, средства компьютерной техники, новейшие информационные технологии активно используют организованные преступные группировки [1], в том числе и для легализации доходов, полученных преступным путем. Эксперты ОБСЕ оценивают ежегодный ущерб для мировой экономики от промышленного шпионажа, воровства и мошенничества в интернете в 100 млрд долларов [2].

Организация безналичных расчетов населения с использованием пластиковых карточек остается быстро развивающейся сферой деятельности российских коммерческих банков. По данным Банка России на 1 августа 2013 года количество кредитных организаций, занимающихся эмиссией пластиковых карт, достигло 661, при этом на территории Российской Федерации эмитировано уже более 205 млн. карт. Только за 2 квартал 2013 года было совершено более 1,8 млрд. транзакций с пластиковыми картами на сумму 6,3 трлн. рублей [3].

При этом ущерб от мошенничества с пластиковыми картами также растет. Ассоциация региональных банков, используя материалы платежных систем VISA и Mastercard, подсчитала, что по итогам 2008 года ущерб от мошеннических операций с пластиковыми картами составил 1 млрд. рублей и по сравнению с прошлым годом увеличился на 206%[4]. В настоящее время, по мнению экспертов, размер ущерба постоянно растет.

Однако точной статистики по количеству мошеннических операций с пластиковыми картами нет, так как данные преступления обладают высокой латентностью. Это связано в том числе с тем, что банки стараются не разглашать информацию о мошеннических транзакциях или тем более о взломах баз данных, так как это может негативно отразиться на их деловой репутации. По оценке специалистов только 15% всех совершенных преступлений попадают в поле зрения правоохранительных органов [5]. Однако неоспоримым является тот факт, что ущерб от мошеннических операций с пластиковыми картами продолжает расти. Кроме того все ярче проявляется транснациональный характер данных мошенничеств.

2. Особенности и виды совершения мошеннических операций с банковскими картами

Исследования правоохранительных органов показали, что наиболее распространенным видом мошенничества с использованием пластиковых карт является мошенничество с использованием поддельных карт и украденных реквизитов действующих карт.

Можно выделить две группы преступлений, совершаемых с использованием пластиковых карт: совершаемые в системе банка, совершаемые вне банка.

К первой группе преступлений относятся: несанкционированная установка на карточку кредитного лимита, позволяющая увеличить авторизационный остаток на карточном счете с последующим снятием средств; несанкционированная установка в авторизационной системе специального статуса счета, позволяющего в определенных пределах снимать средства с карты; выпуск параллельной карты-двойника; несанкционированный выпуск новых пластиковых карт; сговор с представителями торговых точек и др.

В группе преступлений, совершаемых вне банка, можно выделить три группы преступлений: преступления, совершаемые с участием владельца пластиковой карты; преступления, совершаемые с использованием поддельных, украденных карт или идентификационных данных; преступления связанные с несанкционированным проникновением в хранилища данных или путем внедрения в различные устройства.

К случаям мошенничества владельца пластиковой карты можно отнести следующие: мошенничество на долимитных суммах; ложные заявления о краже или утере карточки.

Так, преступник по подложному общегражданскому паспорту на чужое имя получил в консульском отделе МИД России подлинный заграничный паспорт на данную фамилию. По этому паспорту преступник получил в филиале московского банка дебетовую карту «Еврокард/Мастеркард», внеся 5 тыс. долл. США. После этого, находясь на территории Франции, заведомо зная об отсутствии средств на счете, обеспечивающем карточку, он расплачивался ею за товары и услуги, в частности получил напрокат автомобиль, который перегнал в Россию, где продал его по подложным документам. В результате банку причинен ущерб на сумму 22 тыс. долл. США.

Преступления, совершаемые с использованием поддельных, украденных карт и идентификационных данных, можно разделить на следующие виды:

1. Мошенничество с использованием украденных карт.

2. Мошенничество с использованием поддельных карт. Сотрудниками Управления «К» МВД России в 2008 г. пресечена деятельность участников организованной преступной группы, которая на протяжении нескольких лет занималась изготовлением поддельных пластиковых карт и хищением денежных средств со счетов законных владельцев. От преступного бизнеса пострадали как российские банки, так и 8 крупнейших банков Бразилии, Германии, США, Франции и других стран. Все участники организованной преступной группировки являлись активными пользователями сети Интернет и пользователями одного из сайтов, продававшего информацию о реквизитах действующих карт (номерах действующих карт, сроках их действия, Card Verification Value (Card Validation Code)), располагающегося на Кокосовых островах. Один из участников осуществлял неправомерный доступ к серверам процессинговых центров банковских учреждений и копировал информацию о держателях пластиковых карт. Впоследствии данные поступали к организатору, который при помощи термо-сублимационного принтера изготавливал пластиковые карты с магнитной полосой и логотипами банков, и с при помощи специального устройства – «энкодера», записывал похищенную банковскую информацию на пластиковые карты. Используя подделки, участники ОПГ в крупных торговых сетях совершали покупки дорогостоящих товаров, которые в дальнейшем реализовывались, а прибыль поступала в «бюджет» преступного сообщества. За период с января по март 2008 г. зафиксировано 350 финансовых операций, проведенных злоумышленниками. Общий ущерб, нанесенный действиями злоумышленников, превысил 110 миллионов рублей.

3. Мошенничество с использованием карт с частичной подделкой. Так, преступник приобрел пластиковые карточки «Золотая корона» четырех банковских учреждений, затем, используя специальное оборудование, нарушил электронную защиту пластиковых карт и с применением специально разработанного программного обеспечения внес изменения в имеющуюся на них информацию, позволяющие неоднократно получать в банкоматах сумму, свыше находящейся на счете.

В 2009 г. выявлено преступление, в котором для получения наличных денег использовались пластиковые карты. Группа лиц зарегистрировала фиктивную организацию с целью прикрытия незаконной деятельности по обналичиванию денежных средств и уклонения от уплаты налогов. Материальный ущерб, причиненный федеральному бюджету в виде неуплаченных налогов, составил более 105 млн. рублей. В ходе оперативных мероприятия были изъяты регистрационные и финансовые документы, печати более 30 фирм-однодневок, использовавшихся в схемах незаконной банковской деятельности, электронные ключи доступа к системе дистанционного управления счетами «Банк-Клиент», в том числе иностранных организаций, а также неучтенные наличные денежные средства в размере более 2,5 млн рублей, 35 кредитных банковских карт, оформленных на подставных физических лиц, посредством которых снимались наличные денежные средства.

4. «Белый пластик». При использовании данного способа на заготовках пластика стандартного размера злоумышленники эмбоссируют номера действительных пластиковых карт. Магнитная полоса копируется с подлинной карты, например при помощи скимера. Чтобы воспользоваться «белым пластиком» мошенники вступают в сговор с кассирами торгового предприятия, нередко для операций с «белым пластиком» создаются подставные фирмы.

В 2008 г. преступники узнали об уязвимом месте компьютерной защиты компании PBS WorldPay, которая занимается оформлением платежей, в том числе по кредитным и дебетовым картам, находится в Атланте и является подразделением Royal Bank of Scotland. Объектом взлома стали дебетовые карты, привязанные к счетам, на которые работодатели перечисляют зарплату своих сотрудников. За 4 дня преступники (жители Таллина, Кишинева и Санкт-Петербурга) взломали компьютеры PBS и похитили из ее баз

данных номера дебетовых карт и их PIN-коды. Затем они сообщили номера 44 карт и соответствующие коды своим сообщникам в разных странах, которые изготовили фальшивые карты и нанесли на них похищенные данные. Через некоторое время, сообщники начали снимать деньги из таллинских банкоматов и в за несколько часов похитили таким образом около 289 тысяч долларов. Поскольку на счетах законных владельцев карт обычно лежали скромные суммы, обвиняемые заставили компьютеры PBS повысить кредитный лимит, иногда до полумиллиона долларов. В следующие 12 часов из более чем 2100 банкоматов в 280 городах планеты было вынуто примерно 9,5 млн долларов. Исполнители оставляли себе от 30% до 50% похищенной суммы, а остальное отправляли хакерам через компании Western Union и WebMoney[6].

5. Мошенничество торговой точки. Так, кассир магазина, продавая товар за наличные деньги, не оформлял кассовые чеки покупателям. После закрытия магазина, в POS-терминал вводились данные пластиковых карт, которые держатели в течении дня предъявляли к оплате за товары. При этом указывалась сумма, намного превышающая ту, что была получена наличными от покупателей. На слипах кассир подделывал подписи держателей карт, используя в качестве образца чеки, хранившиеся в кассе.

6. Мошенничество с использованием номера счета. Взламывая сети, злоумышленники получают полную информацию о номерах действительных пластиковых карт, сроках их действия и именах держателей. Используя эти данные, они переводят эти средства на счет виртуального магазина или фирмы. Затем под предлогом отказа от покупки оформляется возврат электронных денег на счет преступника, после чего деньги легко обналичиваются.

7. Копирование магнитной полосы (скиминг). Данный вид мошенничества предусматривает использование особых видов устройств, считывающих информацию с магнитных полос карт. Скиммер считывает и записывает информацию на магнитной полосе. Т.е. у злоумышленников появляется данные необходимые для дальнейшего изготовления поддельной карты и ее использования в своих целях.

8. Фишинг, вид мошенничества в результате которого злоумышленникам путем обмана становятся доступны реквизиты банковской карты и пин-код. Чаще всего используется в виде рассылки через Интернет писем от имени банка или платежной системы с просьбой подтвердить указанную конфиденциальную информацию на сайте организации. В России участились случаи появления web-сайтов, на которых предлагаются различные финансовые услуги с использованием платежных (банковских) карт международных платежных систем, таких как VISA и MasterCard. Пользователям предлагается заполнить электронные формы и указать реквизиты платежных (банковских) карт, включая пин-код. При этом передача конфиденциальной информации ведется без использования защищенных протоколов информационного обмена.

9. Вишинг, или голосовой фишинг, вид мошенничества, при котором злоумышленник использует технологию, позволяющую автоматически собирать информацию о реквизитах действующих карт, при котором злоумышленники имитируют звонок автоинформатора, который сообщает, что с его картой якобы производятся мошеннические действия и дает инструкции – перезвонить по определенному номеру. Злоумышленник, принимающий звонки по указанному автоответчиком номеру, представляется сотрудником банка и просит произвести сверку, во время которой и получает все необходимые данные.

К преступлениям, связанным с несанкционированным проникновением в хранилища данных или путем внедрения в различные устройства можно отнести следующие:

1. Использование фальшивых банкоматов. 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 успевают скопировать данные с магнитной полосы карты и его пин.

2. Использование в банкоматах «ливанской петли» – пластиковых конвертов, размер которых немного больше размера карточки , которые закладывают в щель банкомата. При попытке снять денег в банкомате устройство не может считать данные с магнитной полосы, а владелец карты не может извлечь ее. В это время подходит злоумышленник и говорит, что для того, чтобы вернуть карту, надо ввести пин-код. После того как владелец ввел пин-код и так и не смог извлечь карту он уходит, чтобы связаться с сотрудниками банка. Сразу после этого злоумышленник извлекает карту, которую сможет использовать для снятия наличных денег в банкомате, так как ему стал известен пин-код.

3. Взлом баз данных платежных систем и торговых точек. Так, гражданин США при помощи хакерских атак с 2006 по 2008 год похитил данные 130 млн. карт путем взлома платежной системы Heartland Payment Systems, а также данные 4,2 млн карт путем взлома данных супермаркетов Hannaford Brothers Co. и еще двух торговых сетей. Вместе с сообщником хакер устанавливал на взломанных компьютерах программы, которые давали им повторный доступ к системе. Атаки совершались с серверов, находящихся в Нью-Джерси, Калифорнии, Иллинойсе, в Латвии, Голландии и на Украине. На них хранились вредоносные программы, и похищенные данные о картах и их держателях. По предварительным оценкам ущерб превысил 400 млн. долларов[7].

В 2009 г. арестован гражданин Украины, которому за период с 2004 по 2006 год удалось присвоить около 11 млн. долларов с помощью незаконных операций по продаже данных похищенных кредитных и дебетовых карт, преимущественно, граждан США[8].

4. Внедрение вредоносных программ. По данным Федерального бюро расследований США на серверы финансовой компании Citigroup летом 2009 г. была совершена хакерская атака. Следователи выяснили, что пароли клиентов банка были похищены с помощью программы Black Energy, разработанная российским хакер под ником Cr4sh. Пакет с программным обеспечением, в который входит Black Energy, продавался в интернете по 700 долларов. По данным Wall Street Journal, потери клиентов Citibank могут исчисляться десятками миллионов долларов. В частности, у некоего Роберта Бланчарда, совладельца компании Bridge Metal Industries, преступники якобы украли и перевели на счета в Латвии и на Украине миллион долларов[9].

В 2009 г. сотрудниками отдела «К» УВД по Курганской области

пресечена деятельность участников организованной преступной группы, на протяжении двух лет занимавшихся подделкой пластиковых карт, а также хищением денежных средств с банковских счетов с использованием неправомерного доступа к счету через сеть Интернет. Преступники похищали с помощью вредоносных программ ключи электронно-цифровой подписи для получения доступа к банковским счетам, а также данные пластиковых карт граждан. Затем регистрировали фиктивные предприятия и впоследствии оформляли расчетные карты для обналичивания похищенных денежных средств. Ущерб от противоправной деятельности злоумышленников составил около 10 млн. рублей [10].

И это только часть способов, которыми совершаются карточные мошенничества.

3. Направления противодействия преступлениям и правонарушениям с использованием банковских карт

Для борьбы с мошенничеством с пластиковыми картами необходимо принимать всесторонние меры со стороны банков, платежных систем, правоохранительных органов.

Необходимо совершенствовать сами пластиковые карты, увеличивать количество степеней ее защиты, в том числе с использованием чипов, микропроцессорных карт. По данным на середину 2012 г. только 40% карт в России оборудованы микропроцессором [11].

Значительная часть мошеннических операций происходит из-за ненадежности методов идентификации пользователей. Самым распространенным методом является сочетание логина и пароля. Однако для хакеров такой метод не является преградой для свершения мошеннических действий. Необходимо разрабатывать новые системы идентификации пользователей, как например система идентификации пользователя при помощи карт доступа, специальных пластиковых карт с микрочипом, которые вводятся в специальное считывающее устройство, и после этого вводится логин и пароль. При этом микрочип генерирует однократный код, состоящий из 2048 бит, с которым пользователь регистрируется в сети и который уничтожается после того, как пользователь покидает сеть. Такой метод предотвращает любые попытки кражи пароля злоумышленником.

Одной из последних разработок является биометрическая аутентификация пользователя, которая идентифицирует клиента по отпечаткам его пальцев или роговой оболочки глаза. Это делает невозможным доступ в систему злоумышленника, похитившего идентификатор или узнавшего пароль. Однако данный метод является дорогостоящим, что сильно ограничивает возможности по его использованию.

Наиболее уязвимыми местами утечки информации традиционно являются точки подключения к интернету и другим электронным сетям. Именно так в банковскую сеть стремятся проникнуть хакеры. Здесь, как правило, банки устанавливают межсетевые экраны (firewall), фильтрующие сетевой трафик, не допуская несанкционированного проникновения, а также системы Content Security, устанавливаемые на уровне серверов и рабочих станций. Важно проводить мониторинг всех транзакций для выявления мошеннических операций.

Банкам необходимо обеспечить надежность систем защиты информации, регулярно осуществлять контроль за деятельностью сотрудников банка, организовывать проверки оборудования, программного обеспечения и средств защиты баз данных.

При выявлении, расследовании и документальном выявлении эпизодов мошенничества с пластиковыми картами необходимо обратить внимание на следующие признаки, анализ которых может помочь выявлению возможных нарушений со стороны служащих банка:

– отсутствие четкого разграничения функций сотрудников, ответственных за оформление и выдачу пластиковых карт, и сотрудников, ответственных за присвоение персональных идентификационных номеров;

– отсутствие надлежащего контроля за неоформленными пластиковыми картами и ПИН-кодами;

– отсутствие надлежащего контроля за возвращенными почтовыми отправлениями (при рассылке карт по почте);

– отсутствие контроля за увеличением размера овердрафта по счету;

– отсутствие контроля за изменением имен и места проживания клиентов;

– частые сбои в авторизационной системе;

– частые задержки, не вызванные реальной необходимостью, в выдаче клиентам пластиковых карт и ПИН-кодов;

– отсутствие лимита на предельный размер снятия средств через банкомат в течение одного дня.

Для сокращения количества мошенничеств с использованием пластиковых карт банку необходимо принимать следующие меры:

– проводить тщательную проверку контрагентов при заключении договоров эквайринга;

– проводить проверку подлинности документов и сведений, предоставляемых при выдаче пластиковой карты;

– совершенствовать процесс авторизации и идентификационные методы;

– осуществлять проверку кредитной истории держателя карты.

Во всем мире отмечается устойчивая тенденция объединения хакеров в группы, в том числе международные, для совершения крупномасштабных преступлений. В целях сокрытия своей причастности к совершению преступлений злоумышленниками используются похищенные реквизиты доступа в сеть интернет, однократные выходы в сеть с присвоением разных IP-адресов и другие способы электронной конспирации.

Правоохранительным органам необходимо предпринимать меры для организации обмена опытом тесного сотрудничества при выявлении и расследовании данных преступлений. На базе МВД России необходимо создать картотеки по признакам и механизмам подделки банковских карт.

Способы совершения преступлений изменились в связи с появлением новых технических возможностей. Однако уголовное законодательство в данной области не претерпело необходимых изменений. Так, например, сбор и хранение физическим лицом на персональном компьютере данных о действующих пластиковых картах (номерах, сроках действия и даже CVC, включая информацию с магнитной полосы) с точки зрения российского законодательства, не является преступлением или правонарушением. В уголовный кодекс, с нашей точки зрения, необходимо вводить новые составы преступлений.

4. Заключение

Новые экономические реалии, активная интеграция страны в мировую экономику, вступление во Всемирную Торговую Организацию, обусловили острую необходимость повышения конкурентоспособности отечественной банковской системы, что невозможно без внедрения новых технологий и инновационных услуг, которые сопряжены с риском. Возможность реализации этих рисков, а также нарастающие угрозы, связанные с мошенническими операциями в этой сфере банковской деятельности, заставляет банки по-новому взглянуть на проблемы экономической безопасности и искать адекватные, комплексные подходы к отражению рисков и угроз экономической безопасности.

Литература

1. Голубев В. Компьютерная преступность: угрозы и прогнозы //crime-research.ru

2. http://www.bbc.co.uk/russian/russia/2009/12/091214_russia_usa_cyber_security.shtml

3. http://www.cbr.ru/statistics/PrintYG.aspx?Year=2013&pid=psRF&sid=ITM_28382

4. Гуркина Е. Как защитить пластик. //Финанс. – 2009. – №41. – с. 36.

5. www.securitylab.ru

6. www.bbc.co.uk

7. www.bbc.co.uk

8. http://www.ecrimeresearch.org/

9. www.bbc.co.uk

10. www.mvd.ru

11. http://www.mastercard.com/ru/

References

1. Golubev V. Computer crime: threats and forecasts//crime-research.ru

2. http://www.bbc.co.uk/russian/russia/2009/12/091214_russia_usa_cyber_security.shtml

3. http://www.cbr.ru/statistics/PrintYG.aspx?Year=2013&pid=psRF&sid=ITM_28382

4. Gurkina E. How to protect plastic.// Finance. – 2009. – №41. – c. 36.

5. www.securitylab.ru

6. www.bbc.co.uk

7. www.bbc.co.uk

8. http://www.ecrimeresearch.org/

9. www.bbc.co.uk

10. www.mvd.ru

11. http://www.mastercard.com/ru/