# Электронная коммерция и мошенничество в области идентификации личности

*Гарет Джоунс (Gareth Jones) — специалист по борьбе с мошенничеством в области идентификации личности. Возглавляет отдел по идентификационной защите компании Experian. gareth.jones@UK.experian.com*

**В данной статье рассматриваются проблемы личной и корпоративной идентификации в Великобритании, способы повышения идентификационной защиты, а также методы, применяемые мошенниками при создании фиктивных идентификационных документов или их подделке. Интернет используется в качестве канала представления розничных и финансовых услуг, и идентификация крайне важна для этого бизнеса. Кроме того, анализируются возможности и целесообразность мер по борьбе с мошенничеством, направленных на его сокращение и предотвращение повторных атак.**

## Введение

Уровень секретности, окружающей мошенничество в сфере электронных средств связи, в частности Интернета, таков, что в статье не могут быть приведены названия компаний. Однако в ней подробно рассказывается, почему и над чем сейчас трудятся мошенники, как предотвращать подобные преступления и каковы их последствия.

Позволю привести последние цифры по использованию Сети в Великобритании. Они получены в результате исследования 500 тыс. интернет-пользователей, проведенного компанией Experian в рамках программы изучения образа жизни (декабрь 2000 г.). В нем представлен наиболее статистически обоснованный анализ того, как используют Интернет потребители в Великобритании. Кроме того, содержится важная информация о том, как изменился процесс совершения покупок через Интернет за последний год, а также сведения о возрасте онлайновых покупателей, их доходах, частоте совершения покупок и типах приобретенных товаров. Согласно этим данным, количество пользователей, совершающих покупки через Интернет, увеличилось с начала года более чем в 2 раза. Люди стали более активно совершать покупки через Сеть. В частности, с января 2000 г. около 1,5 млн человек совершили не менее четырех покупок. Наиболее популярными приобретениями были книги, компьютерные игры, музыка и туристические путевки.

На основании результатов исследования интернет-пользователей были сделаны следующие выводы:

- количество жителей Великобритании, совершающих покупки через глобальную компьютерную сеть, за последний год возросло более чем в 2 раза: с 5,1% (2,26 млн взрослых людей) — в начале 2000 г. до 10,7% (4,7 млн) — в декабре того же года;
- около 3,3% всего взрослого населения Великобритании (примерно 1,45 млн человек) совершили с начала года по четыре и

**Таблица 1.** Интернет-покупки по товарам

| Покупки | Январь 2000 г., % | Декабрь, 2000 г., % |
|---|---|---|
| Книги | 28 | 29 |
| Музыка | 18 | 21 |
| Туры | 14 | 17 |
| Компьютерные игры | 12 | 12 |
| Видеокассеты | 6 | 7 |
| Одежда | 8 | 6 |
| Вино | 3 | 3 |
| Детская одежда | 2 | 2 |
| Оборудование для огорода | 3 | 2 |
| Финансовые услуги | 4 | 1 |
| Медицинские препараты | 3 | 1 |

более покупок через Интернет, что выразилось в увеличении доли таких активных покупателей с 24 до 34%. А вот количество потребителей, совершивших за тот же период только одну покупку через электронные средства связи, сократилось с 35 до 27%;

- туристические путевки, книги, компьютерные игры и музыка — по-прежнему наиболее популярные товары, и каждая из этих категорий увеличивает свою долю в общем количестве покупок в Сети. Туристические поездки занимают четвертое место в списке наиболее популярных покупок (рост с 14 до 17%). Это увеличение частично объясняется большей прозрачностью и доступностью услуг по резервированию «горящих» путевок или билетов со скидкой от туроператоров и компаний, продающих авиабилеты, при поддержке не только рекламных ATL-кампаний на телевидении и в печатных СМИ, но и в Интернете (табл. 1);
- интернет-покупатели — в основном молодые и состоятельные люди (табл. 2, 3). В сравнении со средней демографией по стране, наиболее широко представленной возрастной группой среди интернет-покупателей являются люди в возрасте 18–25 лет (покупательская активность в 2 раза выше, чем в среднем по стране). Однако существует большое количество интернет-покупателей в возрасте от 26 до 45 лет; люди 26–35 лет также широко представлены — индекс соответствия 166% по сравнению со страной в целом, в то время как 36–45-летние занимают в этом списке пятое место. Исследование выявило значительную покупательскую активность и тех, чей возраст превышает 55 лет. Хотя она составляет лишь половину национальной нормы среди всех интернет-покупателей, представители этой возрастной группы осуществляют 1/5 часть всех интернет-покупок;
- значительный процент интернет-покупателей не считает глобальную компьютерную сеть ценным образовательным ресурсом (37%). Только 22% заявили, что он важен. Оставшаяся часть (41%) выразила нейтральное отношение к этому вопросу.

Результаты исследования Canvasse Lifestyle дают возможность оценить реальный объем рынка онлайновой торговли и темпы роста за последний год. Учитывая, что средняя интернет-покупка оценивается в $50, можно сделать вывод, что объем продаж в Интернете за последний год увеличился более чем в 2 раза (с 264 млн в начале января 2000 г. до 602 млн фунтов стерлингов в декабре того же года).

Согласно этим цифрам, потребители не слишком обеспокоены риском оказаться жертвами мошенников. Между тем по многочисленным публикациям на эту тему создается впечатление, что Интернет является царством беззакония, в котором способны выжить только уверенные в себе пользователи. Более опытным пользователям это, конечно, кажется нонсенсом. При условии, что даже новички спокойно устанавливают себе антивирусные программы и прекрасно осведомлены о своих правах и ответственности по условиям соглашения с поставщиком финансовых услуг,

**Таблица 2.** Интернет-покупатели — срез доходов

| Годовой доход, $ | Процент | Национальная норма, % |
|---|---|---|
| 0-19 тыс. | 33 | 65 |
| 20-39 тыс. | 42 | 27 |
| 40-60 тыс. | 16 | 6 |
| Более 60 тыс. | 9 | 2 |

**Таблица 3.** Интернет-покупатели — возрастной срез

| Годовой доход, $ | Процент | Национальная норма, % |
|---|---|---|
| 18-25 | 9 | 4 |
| 26-35 | 27 | 17 |
| 36-45 | 25 | 20 |
| 46-55 | 19 | 18 |
| Более 55 | 20 | 41 |

Интернет является относительно безопасным и интересным местом для взаимодействия. Одним словом, транзакции с участием «виртуальных компаний» практически не связаны с риском стать жертвой мошенничества для покупателей. Однако проведение торговых операций через Интернет — совсем другое дело. Существует множество различных способов обмана компаний-продавцов, и ровно столько же возможностей предотвратить их. В конечном итоге соотношение между риском и реальными случаями мошенничества зависит от умений и навыков настоящих и потенциальных «преступников», а также от защитных мер, предпринимаемых потенциальными жертвами.

Дальнейшие размышления больше похожи на программу действий по борьбе со вселенской угрозой. Прежде всего, рассмотрим, что собой представляет идентификация, ее место в Интернете, причины и возможные альтернативы. Затем проанализируем, как осуществляется мошенничество с позиции потребителей и компаний. Любой читатель, которого интересует вопрос о незаконных действиях, должен сначала прочитать раздел, посвященный мерам предотвращения мошенничества, иначе его схемы окажутся недолговечными! Наконец, последнее. Мы расскажем о проблемах частного права, которые должны затрагиваться в любой статье по идентификации и мошенничеству. Все это касается двух рынков — финансовых услуг и электронной коммерции — по одной простой причине: именно на них все и происходит.

### Что такое идентификация?

Идентификация — чрезвычайно широкое понятие. Оно включает в себя личные данные: происхождение (при смене имени), дату и место рождения, адрес и даже кодированные ссылки на самих себя. Действительно, в некоторых организациях нас идентифицируют скорее номерами и кодированными ссылками, чем по имени и месту жительства. Организации имеют разные точки зрения относительно того, какие характеристики должна содержать идентификация. В частности, на рынке финансовых услуг это регулируется определенными правилами. В каждой стране идентификационные характеристики различны.

Великобритания отличается от других государств тем, что у нее нет национальной идентификационной карты или иного всеобщего удостоверения личности. Личность может быть объективно идентифицирована через материалы, в которых содержатся ссылки на идентификационные характеристики, и через совокупность наиболее убедительных из них. Подтверждение идентификации, таким образом, представляет собой сбор информации, касающейся событий жизни и истории данного субъекта. Сведения по отдельности не обеспечивают подтверждения идентификации, однако при их объединении данные становятся более убедительными.

В этом и состоит суть проблемы. Цель идентификации в идеале — достижение абсолютной уверенности в том, что покупатель является именно тем, за кого он себя выдает. Однако реальность такова, что степень уверенности зависит от того, записываются ли идентификационные характеристики и доступны ли они в некотором хранилище. Таким образом, главной проблемой является наличие методов, позволяющих оценить показатели уверенности при идентификации покупателя.

Надежность показателя уверенности будет подкреплена (или, напротив, ослаблена) способностью компаний получить личностные характеристики покупателей, полезные для их безошибочной идентификации. Это весьма актуально в настоящее время, поскольку самозванцам — тем, кто выдает себя за других лиц, — часто не удается точно повторить идентификационные характеристики «низшего уровня» реального лица (в частности, предыдущее место жительства, рабочий телефон, время проживания по этому адресу и дату рождения). К тому же им неизвестна частная информация, например номера или детали финансовых счетов, открытых реальными лицами и пр.

Таким образом, оценка идентичности заключается в выполнении двух задач — «обоснования» и «подтверждения». Первый шаг — проверка того, что данное лицо существует, второй — сопоставление его с идентификационными данными. При определении критериев надежности необходимо разложить на множители риск, связанный со справочными материалами. Следует также рассмотреть методы отбора коммерческих и государственных организаций, в которых накапливается материал о случаях мошенничества и подделок, а также форму связи с лицами, представляющими эти данные.

Безусловно, как потребители мы рассчитываем, что строгость процессов идентификации будет соразмерна с целью идентификации. Мы не рассчитываем на полную идентификацию при осуществлении простых операций, например, при получении новых финансовых услуг. Вопрос оценки идентификации покупателей важен, поскольку, несмотря на то, что транзакции могут быть первоначально авторизированными, ложная идентификация неизбежно ведет к потерям и убыткам розничных компаний. При оказании финансовых

услуг борьба с ложной идентификацией важна по двум причинам: она позволяет предотвращать мошенничества (которые неизбежно приносят убытки), и способствует борьбе с отмыванием денег. Таким образом, уровень доверия, который выбирают компании при оценке тождественности покупателя, зависит от условий того или иного рынка.

Большинство компаний имеют собственную систему идентификации. Те из вас, кто изучает право, вспомнят дело Solomon vs Solomon, когда было выяснено, что ряд крупных корпораций имеет собственную легальную идентификацию, не имеющую ничего общего с их идентификационными данными сотрудников. Мелкие компании не привязаны к идентификационным характеристикам своих владельцев, поэтому по юридическим соображениям подчас считаются самостоятельными физическими лицами. При оказании финансовых услуг организации идентифицируются на личностном уровне обычно в ходе проверки тождественности директоров. В этом случае идентификационные характеристики компании и индивидуума оцениваются одинаково.

Почему так важна идентификация? Почему мы так об этом беспокоимся? Это важные вопросы, поскольку они являются ключом к нашему статусу, квалификации, правам и привилегиям, которые нам дали или которых мы добились сами. Все эти характеристики делают нас уникальными и позволяют объективно оценить нашу работу, пристрастия, профессию, способности, интересы и, в конечном итоге, нашу стоимость и ценность. Таким образом, наша идентичность является одной из наиболее дорогих вещей, которая у нас есть, и атаки мошенников на доверие воспринимаются нами близко к сердцу и причиняют особую боль. Если это случается, возникает ощущение криминальной клеветы на нашу личность. Сам факт того, что от нашего имени было сделано что-то нам неизвестное кажется менее важным, чем то, кто это сделал, — именно так думают люди. Для жертвы идентификационного мошенничества самое важное — избежать упреков в действиях, которые он или она на самом деле не совершали. Для жертв чрезвычайно важно, чтобы их отличали от «подозреваемых», чтобы люди, отвечающие за хранение идентификационной информации, делали это ответственно и защищали доверивших им свои данные от атак, злоупотреблений и мошенничества. Это является и юридическим требованием в соответствии с принятым в 1998 г. Законом о защите информации.

Подлинная идентификация клиентов так называемых «доткомов» (онлайновых компаний) важна, поскольку ценность этих компаний может быть определена в соответствии с размером и надежностью их покупательской базы. С ее помощью «виртуальные компании» имеют возможность сегментировать, продвигать свои товары на рынке и вести перекрестные продажи. Таким образом, значительно возрастает и уровень доверия к идентификации личности покупателей.

Идентификация компании имеет не меньшее значение, поскольку к имени добавляется субъективный уровень доверия покупателя к честности организации и качеству товаров и услуг. Нередко субъективный уровень доверия заменяется объективным от третьей стороны. Чтобы укрепить доверие покупателей к новым и существующим компаниям, специализирующимся на электронной коммерции, были предложены схемы проверки честности организации, скрывающейся за страничкой в Интернете.

Получение деловой информации об организации и ее директорах — еще один способ доступа к данным, касающимся репутации компании и повышения доверия к ней.

Идентификационные характеристики могут быть скопированы или фальсифицированы. Поскольку уровень мошенничества зависит от сегмента рынка, данная проблема заслуживает некоторого объяснения. Знание механизмов фальсификации позволяет нам разработать такую процедуру, которая определит и даже предотвратит ситуации, чреватые финансовыми потерями. Оно также дает нам возможность смягчить реакцию «хороших» покупателей на предпринимаемые меры по предупреждению мошенничества. Бремя операционных расходов по идентификации выходит в данном случае на первое место. Это особенно важно в розничном секторе, где минимальные стандарты безопасности не прописаны в единых инструктивных документах, а непрозрачные методы могут оттолкнуть «хороших покупателей», поскольку увеличивают накладные расходы компании и в результате — цены.

Раскрытие подлинной идентификации не является универсальной нормой в нашей обычной жизни. В реальном мире идентификация при денежных транзакциях — не проблема, так зачем говорить о ней? В виртуальном мире, в чатах принято использовать псевдонимы — «ники». Вряд ли это изменится в будущем, хотя и таит в себе ряд опасностей, поскольку анонимная природа Интернета как среды позволяет тем, кто этого сильно хочет, представить о себе ложную информацию.

### Методы совершения мошенничества

Частота столкновений добропорядочных компаний с мошенничеством разная в розничной торговле и финансовых услугах. Как правило, в

среднем проблемные транзакции составляют небольшой процент от оборота, однако на некоторых рынках их доля может достигать значительных размеров. В области электронной коммерции и финансовых услуг имеется достаточно данных об активности организованной преступности, подтверждающих, что криминал активно осуществляет при помощи Сети свои преступные замыслы, в том числе распространение порнографии и наркоторговлю. Таким образом, мошенники подчас оказываются преступниками, нарушающими закон. Они не заслуживают названия «белые воротнички», так часто употребляемого по отношению к ним.

Невозможно полностью описать все методы совершения мошенничества в области идентификации личности, остановимся только на основных проблемах. В связи с многогранной природой мошенничества на рынке финансовых услуг и розничной торговли, важно разделить методы совершения преступления на секторы. Прежде всего, рассмотрим транзакционное мошенничество в отношении бизнеса, затем идентификационное мошенничество в области финансовых услуг и мошенничество в идентификации бизнеса.

### Транзакционное мошенничество

Это обман розничных торговцев, при котором их заставляют поверить в то, что преступники имеют право на пользование пластиковой карточкой (кредитной или дебетовой). Преступник имеет выбор: воспользоваться именем владельца карточки, именем третьей стороны или вообще вымышленным именем. Решение зависит от того, есть ли у него доступ к информации о настоящем владельце карточки и как будет организована идентификация при получении товаров, а также от общего уровня проведения преступных операций. Преступники зачастую настолько уверены в несовершенстве методов предотвращения подобного рода операций, что почти не тратят время или усилия на то, чтобы замести следы. Менее 10% из них беспокоятся о переадресации доставки товаров, только 10% — пытаются создать вымышленные телефонные счета.

Наиболее распространенные методы совершения транзакционного мошенничества (по степени актуальности) следующие:

- использование настоящего имени по реальному адресу, но не имени владельца карточки;
- использование имени владельца карточки по реальному адресу, но не по адресу владельца карточки;
- использование ложного имени по реальному адресу;
- использование подлинного имени и адреса владельца карточки, но с доставкой товаров по другому адресу.

Исследование показало, что наиболее распространенным сценарием мошенничества без карточки является «использование настоящего имени по реальному адресу, но не имени владельца карточки (и адреса)». Другими словами, преступник указывает имя реального человека, которое в прошлом ассоциировалось с подлинным адресом, а номер карточки соответствует другому лицу и адресу. Это свидетельствует об уязвимости метода идентификации реального человека и о необходимости «соединить» номер карточки с подлинным адресом проживания ее владельца.

Согласно другой, достаточно распространенной форме мошенничества, — когда используется имя владельца карточки по реальному адресу, но не по адресу ее владельца, — преступники указывают имя, совпадающее с именем на карточке, но адрес не совпадает с адресом выставления счетов. Это говорит о необходимости связывать номер карточки с адресом выставления счетов ее владельцу.

Такой прием, как «вымышленное имя по реальному адресу», тоже был довольно популярной тактикой. Однако она работала до тех пор, пока розничные компании не начали проверять, имеются ли указания на данного человека по различным информационным ресурсам. Это подтверждается и результатами исследований.

Наконец, последний прием — когда указываются подлинное имя и адрес владельца карточки, а посылка доставляется в другое место. С такой проблемой сталкиваются специализирующиеся на интернет-торговле компании при доставке товаров по адресу, отличному от адреса выставления счетов владельцу карточки. Во многих случаях, например, при доставке подарков, подобные операции оказываются настоящими, но сам процесс провоцирует возникновение противоправных действий. Это наиболее легкий способ обмана компаний, специализирующихся на интернет-торговле. С распространением системы контроля за адресами эмитентов карточек (соотносящей номер карточки с адресом доставки счетов владельцу карточки в момент авторизации) такой метод наиболее предпочтителен для преступников, совершающих дистанционные транзакции.

Несмотря на то, что получить номера кредитных карточек из использованных чеков, балансовых отчетов, которые зачастую просто выбрасываются в мусорное ведро, с помощью программного обеспечения по сбору номеров

кредитных карточек — отнюдь не сложная задача, получить реальные имя, адрес владельца карточки и выяснить срок действия карточки — гораздо сложнее. Однако, как только установлен срок действия одной карточки, преступники понимают, что номера других карточек, являющихся продолжением предыдущей, имеют аналогичный срок действия. Это расширяет базу надежной информации для совершения преступления.

Программное обеспечение по сбору номеров кредитных карточек, доступное в Интернете, является главной причиной проблем транзакций без использования карточек. Действительно, способность пользователей Сети позиционировать себя анонимно среди других пользователей и на интернет-страничках создает неразбериху в области идентификации: ведь получить доказательства фальшивой идентификации через этот канал несложно (см. phatism.com).

С распространением систем контроля за адресами эмитентов карточек преступники станут более изощренными, определяя, по крайней мере, правильный адрес владельца карточки или, как только они поймут принципы работы системы, у них появится возможность сопоставлять почтовые адреса с численным значением, захватывать счета или использовать адрес третьей стороны для доставки товаров. Виртуальные товары и услуги не будут создавать больших проблем, так как мошенники могут скопировать правильный адрес владельца карточки, поскольку товары «виртуальны», а связь между IP-адресом компьютера и реальным, физическим адресом может быть скрыта.

Другие способы получения достоверных данных о владельце карточки основаны на взломе интернет-сайтов. Это позволяет осуществлять копирование с относительной легкостью. Последствия таких атак ужасны как для непосредственных, так и для случайных жертв. Непосредственные жертвы — подлинные владельцы карточек — обычно теряют доверие к пластиковым карточкам и сокращают расходы на них. Однако по Закону о потребительском кредите они защищены и в действительности никогда не несут финансовых убытков. Компании, специализирующиеся на торговле через Интернет, на чьи сайты проникли хакеры, рискуют потерять многих покупателей. Это может нанести удар по их будущим продажам в Сети. Эмитенты карточек страдают от операционных издержек по выпуску пластиковых карточек, отзыва денег владельцами карт и снижения прибыли от взимаемых комиссионных в связи с сокращением использования карточек.

### Финансовые услуги и идентификационное мошенничество

Получение преступным путем финансовых услуг вынуждает преступников вести активный поиск, при этом добыча может оказаться больше, чем при транзакционном мошенничестве. Объектами идентификационного мошенничества и имитации становится все то, что позволяет преступнику в итоге получить наличные деньги или товары. Наиболее популярными являются всевозможные формы кредитов — розничный или карточный, ссуды или соглашения о финансировании операций с существующими активами (сдача в аренду). Это обусловлено прежде всего тем, что получаемые продукты — наличные деньги, товары, которые могут быть проданы за деньги, или товары, которые можно конвертировать по высокой цене, например, автомобили и мотоциклы.

### Как совершается идентификационное мошенничество?

Существует множество методов совершения преступления, однако все их можно разделить на две категории: имитация, или копирование, когда преступники используют идентификацию другого лица — настоящего или умершего; разработка вымышленных идентификационных характеристик.

Имитация может быть трех видов:

- «имитация текущего адреса»;
- «имитация предыдущего адреса»;
- «имитация умершего лица».

«Имитация текущего адреса» означает, что преступники копируют идентификационные характеристики реального лица: при заполнении формы они указывают адрес, по которому проживает или проживал ранее данный человек. Преступники с высокой точностью воспроизводят идентификационные характеристики своих жертв — как правило, имя и адрес. Зачастую при этом им не удается воссоздать дату рождения, время проживания по адресу, предыдущее место проживания и другие автобиографические сведения, касающиеся, например, мест работы. Это позволяет, в свою очередь, кредитным организациям, являющимся пользователями различных информационных систем, разработать систему выявления несоответствий и определения случаев мошенничества.

«Имитация предыдущего адреса» — более распространенная форма преступления. Преступники копируют идентификационные характеристики человека, по-прежнему проживающего по данному адресу, который они указывают в заявлении как «предыдущее место жительства». Конечно, они укажут его как свой «текущий адрес», но скажут, что проживали по нему только короткое

время. Подробности кредитных операций, таким образом, сохраняются, и преступник «использует» их, чтобы показать кредитоспособность.

«Имитация умершего лица» — менее распространенная форма преступления, однако когда она применяется, то результаты не заставляют себя ждать. Это такая форма обмана, о которой писал в своей книге «День Шакала» Фредерик Форсайт (Frederick Forsyth). Она предусматривает копирование идентификационных характеристик умершего лица. Умершим часто оказывается ребенок, который родился в то же время, что и самозванец. Подобная информация зачастую берется прямо с кладбищ. Преступник получает свидетельство о рождении на имя ребенка и использует его для других документов, например паспортов или водительских удостоверений. За свидетельствами о рождении закреплено название «генератора документов», их могут использовать для получения других бумаг. Если умерший был взрослым человеком, то преступник имеет возможность заполучить биографические данные из идентификационных характеристик, но он редко используют дату рождения, поскольку характеристики могут относиться к пожилому человеку, а преступник — молодой. Они более подвержены риску быть раскрытыми по целому ряду причин, но, как правило, имя умершего лица вместе с датой рождения на заявлении относится к очень давним временам.

### Создание идентификационных характеристик

Это именно тот случай, когда преступник не копирует идентификационные характеристики другого лица, а для создания иллюзии существования реального лица использует псевдоним. Он может осуществить это через фальшивое включение себя в избирательные списки, создание коммунальных счетов и получение соответствующих документов, используя их в дальнейшем как доказательства для предоставления финансовых услуг. Это, в свою очередь, позволяет ему иметь необходимое количество физических материалов, которые помогут ему в будущем увереннее себя чувствовать под вымышленным именем.

Если преступнику вдруг понадобится конкретный вид доказательства, который нельзя получить в оригинале, он может использовать фальшивку. Современное сканирующее оборудование и программное обеспечение позволяют домашним пользователям изменять документы и создавать подделки. Более организованные профессиональные преступники используют программу Post Office, чтобы дистанцировать себя от места совершения преступления.

Каждый из описываемых в статье методов имеет свои сильные и слабые стороны. В частности, некоторые методы преступлений легче определить финансовым организациям, чем другим. Конечно, существует много различных форм мошенничества, касающихся заполнения документов, но все они относятся скорее к манипуляциям с положением в обществе, чем к идентификационным характеристикам. И по этой причине на них мы не будем останавливаться.

Кто совершает мошенничество? Как выглядят эти люди? В каком направлении развивается эта область правонарушений? Данные говорят о том, что преступники, как правило, являются выходцами из неблагополучных городских районов, хотя бывают и исключения. Адрес, по которому в настоящее время живет преступник, отличается от адреса жертвы. В этом нет ничего удивительного — зачем преступнику копировать идентификационные характеристики человека, у которого плохая кредитная история? Возраст мошенников сильно различается. Это неженатые мужчины, безработные и скорее квартиросъемщики, чем владельцы квартир. Их преступления сравнительно скоротечны, большинство из них раскрывается в течение нескольких месяцев (чаще в течение года). Все зависит от профессионализма преступника и его желания «усыпить» идентификационные характеристики, чтобы создать иллюзию порядочного покупателя, получить и использовать услуги, которые предлагаются им через вертикальные каналы продаж, а затем за короткое время опустошить счета.

Приведем примеры транзакционного мошенничества, идентификационного мошенничества при составлении документов, а также опишем случаи, когда фальшивые идентификационные документы обнародовались:

- пять человек были арестованы в Москве по обвинению в краже номеров кредитных карточек у компаний, специализирующихся на интернет-торговле, и получении по ним 500 тыс. фунтов стерлингов. По данным правоохранительных органов, преступники украли номера более пяти с половиной тысяч карточек путем взлома интернет-сайтов4;
- Nicholas van Hoogstraten, один из наиболее скандально известных владельцев недвижимости, скрывших около 200 млн фунтов стерлингов своего состояния под десятком вымышленных фамилий. Этот человек использовал поддельные удостоверения личности для управления компанией в качестве директора;

- у тысяч владельцев кредитных карточек были похищены их номера, когда они платили за интернет-порнографию. Компании NatWest и Barclays проводят расследование жалоб клиентов о том, что к ним приходят странные счета за порнофильмы. Эксперты компаний полагают, что преступники получают информацию о кредитных карточках не без помощи современной компьютерной техники, а порнофильмы покупают через американский телеканал RJB Telecom;
- газета Observer описывает преступную деятельность Фионы Монт (Fiona Mont) «...Это 30-летняя девушка из богатой и респектабельной британской семьи. Она находилась в бегах, после того как якобы умерла в январе. Она вполне законно имела несколько паспортов на разные имена, чтобы скрыть свою настоящую фамилию. После официальной смены фамилии она выслала старый паспорт и получила взамен новый. Любой человек вправе менять фамилию столько раз, сколько ему заблагорассудится. Правоохранительные органы не предполагают, что порой за этим может стоять преступный умысел. Она использовала различные вымышленные имена, в частности, Франсес Монтгомери (Frances Montgomery), Алисон Миллер (Alison Miller), Джакулина Мейхю (Jacqueline Mayhew) и Джамина Чадмик (Jamina Chadwick);.
- человек, которого обвиняют в мошенничестве, обставляет свою смерть как суицид и бежит в США. Карл Хилдербрандт (Carl Hilderbrandt) получил паспорт при помощи копий свидетельства о рождении умершего ребенка точно так же, как это описывается в романе Фредерика Форсайта (Frederick Forsyth) «День Шакала» (The Day of the Jackal). Его раскрыли во Флориде после того, как его узнал один турист из его родного города Йоркшира в Англии. Во время судебного разбирательства 42-летний Карл Хилдербрандт признался в краже, незаконном получении паспорта и в том, что он скрывался от властей. Первоначальные обвинения в мошенничестве против него не выдвигались. Карла Хилдербрандта приговорили к пятнадцати месяцам тюрьмы, но вскоре он выйдет на свободу, так как уже провел в заключении восемь месяцев;
- газета Bristol Evening Post сообщала, что некий мошенник решил поиграть на горе Кристины Кук (Christine Cook), выдавая себя за ее умершего сына Пола. Преступник использовал удостоверение личности на имя г-на Кука, чтобы сбить полицию со следа, всякий раз, когда она останавливала его за нарушения правил дорожного движения. В результате этого госпожа Кук получала постоянные письма из полиции. Самозванец нанес первый удар через пятнадцать лет после смерти г-на Кука.

### Мошенничество в идентификации бизнеса

Возвращаясь к мошенничеству в области электронной коммерции, необходимо отметить случаи (хотя и немногочисленные), когда покупателей вводят в заблуждение, создавая иллюзию, что они взаимодействуют с реальными компаниями, на самом же деле им предлагают лишь поддельные похожие копии. Такое мошенничество заключается в получении доступа путем обмана (ситуация, когда мошенник так или иначе подменяет в Интернете, на proxy-сервере или брандмауэре, реальный адрес компании на ложный IP-адрес). В частности, преступник загружает ложный веб-сайт, очень похожий на сайт реальной компании, для получения информации о покупателях и их карточках, чтобы впоследствии совершить транзакционное преступление. Многочисленными жертвами становятся люди, которые непреднамеренно сообщают информацию о себе преступникам, пребывая в полной уверенности, что они общаются с респектабельной и хорошо известной фирмой. Настоящие компании, потерявшие новых покупателей из-за шумихи в прессе, могут потерять еще больше потенциальных клиентов из-за недоверия и «подмоченной» репутации. Эмитенты пластиковых карт столкнутся с сокращением расходов потребителями и последующих комиссионных из-за того, что реальные покупатели потеряют доверие к их продуктам.

### Масштабы проблемы

Фактические и возможные потери, возникающие при мошенничестве во время заполнения документов, зависят от степени мер по его предотвращению в момент открытия счета. Практически все банки и другие кредитные институты имеют в своем распоряжении современные системы, позволяющие достаточно легко обнаруживать поддельные документы. Большинство из них является членами объединений, которые делятся друг с другом информацией, чтобы не допускать повторения атак преступников. Разумеется, эти меры не всегда эффективны, однако многим организациям удается предотвратить более 90% преступлений. Уровень пресечения

преступлений достаточно высокий, именно его целесообразно поддерживать всем игрокам на рынке. Что касается доли преступлений с подделкой идентификационных характеристик при заполнении форм, то она незначительна: в среднем для каждой компании в прошлом году около 0,03% всего объема совершаемых преступлений. Преступления общего характера более широко распространены, однако их процент пока еще невелик.

Ассоциация услуг по клирингу платежей (Association for payment Clearing Servises) сообщает о значительном увеличении случаев транзакционного мошенничества: с 135 млн в 1998 г. до 189,4 млн фунтов стерлингов в 1999 г. К маю 2000 г. общие убытки от подделок карточек возросли на 53% и достигли 226 млн фунтов стерлингов. Количество преступлений без использования карточек, охватывающих дистанционные транзакции (не только связанные с электронной коммерцией), возросли на 146%, убытки достигли 40 млн фунтов стерлингов. По данным осведомленных источников, к маю 2001 г. эти цифры вырастут до $300 млн фунтов стерлингов. Промежуточные данные подкрепляют такие прогнозы.

Компании, специализирующие на интернет-операциях, в отличие от банков, сообщают о различных уровнях мошенничества, совершение некоторых из них в процентном соотношении к общему объему достаточно высокое. Эта цифра увеличится, если учесть, что количество заказов мошенников в два раза превысит стоимость «нормальных» заказов. Исследование компании Experian, проведенное в августе 2000 г., в котором анализировались 800 «виртуальных» компаний, так называемых доткомов, показал, что 20% из них несут от мошенников убытки в размере более 1%; 48% компаний сообщили о цифре 0-0,5%; 8% признали убытки 0,5–1,0%. Необходимо также отметить, что есть неофициальные данные о более высоком уровне убытков на некоторых сегментах рынка электронной коммерции (см. вышеупомянутые свидетельства о транзакционном мошенничестве), при этом 23% «виртуальных компаний» отказались раскрыть потери, которые они ожидают понести. Без всякого сомнения, это чрезвычайно щепетильный вопрос, и касается он доверия не только к опрашиваемой компании, но и к каналу в целом. Интересно заметить, что гораздо более высокий уровень мошенничества ощущался, когда владельцами карточек были иностранцы, — 23% опрашиваемых признали, что уровень мошенничества для этих покупателей превышал 10%.

**Решение**

Несмотря на общепризнанное утверждение, гласящее, что мошенничество никогда не будет полностью побеждено, компаниям необходимо проанализировать расходы по предотвращению мошенничества относительно текущих убытков. Существует множество методов и систем по предотвращению транзакционного мошенничества и мошенничества при заполнении документов, различных по эффективности, однако их реализация и обеспечение могут обойтись дороже.

Если обратиться к транзакционному мошенничеству, то существует три уровня его предотвращения. Первый — розничные компании и компании, специализирующиеся на интернет-операциях, второй — провайдер-посредник, обеспечивающий оплату, третий — эмитент карточек. Розничные компании находятся с внешней стороны проблемы и поэтому лучше всего готовы для идентификации нового покупателя. Они могут контролировать задаваемые вопросы, что приводит к проверке идентификации личности. Затем они проверяют, является ли новый клиент «объектом информации», которая получает реальное подтверждение. В итоге они могут быть уверены в удостоверении личности нового клиента и в некоторой степени — в качестве осуществляемой транзакции.

Чтобы получить надежную информацию, обработать ее, создать систему проверки, розничные компании требуют согласия покупателя и коммерческого соглашения с компанией, занимающейся проверкой данных и кредитоспособности покупателя. Принципы взаимодействия должны быть оговорены, данные о покупателях могут использоваться для идентификации и предотвращения мошенничества другими компаниями, предоставляющими данные для этих целей. Такое решение имеет много преимуществ. Не менее важны охват информации, корректирование результатов с помощью критической интерпретации данных. Это также позволяет интегрировать другие продукты, например ранжирование покупателей. Таким образом, вы знаете, кто является клиентом. Его наклонности и пристрастия могут быть более точно прогнозируемы.

Исследование «виртуальных компаний», выполненное фирмой Experian, показало, что хотя банки данных о гражданах активно использовались, чтобы отличить честных покупателей от преступников, лишь 52% опрашиваемых воспользовались этими сведениями. В табл. 4 представлены наиболее популярные источники, используемые для проверки идентификации личности.

**Таблица 4.** Данные, используемые для подтверждения идентификации личности

| Источники | Количество, % |
|---|---|
| Почтовый адрес | 61 |
| Избирательные списки | 39 |
| Телефонные базы данных | 32 |
| Банковские счета | 12 |
| Интернет-сайты BT.com/192.com | 19 |
| Внутренние базы данных | 3 |
| Третья сторона для проверки | 3 |
| Прочие | 3 |

Без сомнения, преступники смогут подделывать эти бумаги по отдельности. Более решительные меры по предотвращению мошенничества, требующие широкого спектра открытых и закрытых данных о пользователях, лучше предотвращают возможные случаи мошенничества. По крайней мере, розничные компании и компании, специализирующиеся на интернет-операциях, признают необходимость быть чрезвычайно внимательными в этой сфере, которая очень ценится организациями, задействованными далее в транзакционной цепочке. Некоторые компании по услугам оплаты предлагают решения и розничным компаниям, и тем, кто специализируется на интернет-операциях. Данные решения идентифицируют ряд преступлений по видам транзакций, которые в соовкупности кажутся подозрительными. В этом есть рациональное зерно, однако опыт показывает, что включение в процесс внешних, не транзакционных, данных все-таки более эффективно.

Систематическое предотвращение случаев мошенничества — широко распространенное явление в среде эмитентов пластиковых карточек. Для этого используется система Falcon, позволяющая идентифицировать все подозрительные транзакции. Для выяснения обычных примеров осуществления транзакций владельцем карточки и, как следствие, нестандартных операций, не соответствующих нормальному покупательскому поведению владельца карточки применяются нейронные сети. Кроме того, данная система дает возможность идентифицировать часть случаев дистанционного мошенничества. Парадоксально, но факт — одним из наиболее вероятных последствий применения этой системы является увеличение числа мошенничества, связанного с заполнением документов (т. е. когда убытки понесет эмитент, а не покупатель).

Меры по предотвращению мошенничества при заполнении документов, как правило, представляют собой сумму данных, распределенных с помощью информации о статусе заявителя, не затрагивающей положение, и ручных систем. Обмен данными — широко распространенное явление в этой области. На рынке доминируют системы CIFAS, Hunter, Detect. Первая из названных существует уже более десяти лет, и ее члены размещают важную информацию об известных случаях мошенничества в базу данных, общую для организаций-членов, в частности, Experian, Equifax и MCL Software. Эта система предотвращает совершение повторных атак из одного и того же источника, и большинство крупных кредитных организаций вместе с представителями из других отраслей экономики вступили в нее в качестве членов. Другой системой обмена данными по принципу статуса является National Hunter, разработанная компанией MCL Software. Она основана на сопоставлении анкетных данных в условиях обработки информации всех членов системы в режиме запаздывания по времени. Локальные системы Hunter дают пользователям определенный свод правил, позволяющих распознавать подозрительные анкетные несоответствия и статус, который соответствует анкетным данным самого пользователя. Система Detect компании Experian дает возможность предотвращать мошенничество в режиме реального времени в Интернете и не только соотносить данные и выявлять несоответствия относительно общей базы данных, но и усиливать преимущества от членства в комитете. Через получение доступа к общим кредитным счетам, поиску кредитов и общественных данных, в частности, избирательных списков, информации о банкротствах, судебных решениях, она контролирует кредитные вопросы. Результат этого процесса представлен в форме «индекса мошенничества», т. е. показателя, который более предсказуем, чем системы, основанные на правилах. Обе системы — Hunter и Detect — интегрированы с системой обмена данными CIFAS, потому в некотором смысле все системы поддерживают друг друга.

Для компаний, занимающихся торговлей через Интернет, чрезвычайно важно быть уверенными в том, что их покупателями являются те, за кого они себя выдают, и обеспечивать безопасность и условия предотвращения мошенничества. Разрабатываются новые системы и процедуры для подтверждения идентификации личности и отслеживания мошенничества в идентификации личности. Яркий тому пример — деятельность компании Experian, использующей процессинг системы Detect для индекса идентификации личности, который отражает уровень доверия к новых клиентов. Существуют и другие методы, в том числе

изучение вызовов преступников и ответной реакции их жертв, а также доказательств идентификации личности через деятельность.

Ручные методы предотвращения преступлений, телефонные проверки домов заявителя или сотрудника широко распространены, поскольку являются необходимым условием для предоставления документальных доказательств идентификации личности вместе с проверками, направленными на предотвращение мошенничества. В государственном секторе обычно принято основываться на справках для подтверждения удостоверения личности заявителя, что является еще одной формой ручного процесса.

Способы защиты информации о покупателях от несанкционированного доступа применяются в некоторых компаниях, однако новизна технологий и недостаток опыта в эксплуатации таких систем сказываются на количестве взломанных вебсайтов. Проблемы обычно возникают в результате плохого обеспечения защиты конфиденциальной информации о покупателях.

### Частная жизнь

Опасность, которая подстерегает системы предотвращения мошенничества, заключается в том, что борьба с преступлениями в этой сфере вступает в конфликт с правом покупателя на личную жизнь. Увеличение объема дистанционных транзакций означает, что все больше и больше личной информации будет обязательно собираться и накапливаться в коммерческой сфере, поэтому необходимо создать систему ее защиты для охраны прав покупателей.

Опасности слишком очевидны. Роберт Шир (Robert Scheer), журналист американской газеты Los Angeles Times и директор проекта частной жизни в университете южной Калифорнии (University of Southern California) написал в журнале Internet Life: «Любой, кто хочет потратить несколько баксов и немного времени на Интернет, сможет узнать о том, что вы читаете, думаете, как зарабатываете, гораздо больше, чем Иосиф Сталин или Адольф Гитлер могли узнать о гражданах своих тоталитарных стран». Он полагает, что право на частную жизнь в Интернете не соблюдается. В той же статье Скотт МакНили (Scott McNealy) из компании Sun Microsystems заявил: «Ваша частная жизнь открыта для всех — не смущайтесь», словно это и есть та цена, которую нам стоит заплатить за чудеса персонифицированного маркетинга.

В Великобритании Закон о защите информации от 1998 г. формирует новую законодательную базу по легитимному поддержанию и обработке данных. Для крупных игроков типична практика прямого взаимодействия с комиссией по защите информации или через торговые ассоциации, интерпретирующая Закон согласно требованиям комиссии. Таким образом, по крайней мере, обработка информации становится легитимной, и права объекта сбора информации защищены. Конечно, глобальная компьютерная сеть является международным феноменом. Наши права в Великобритании заканчиваются на пляжах, и, скорее всего, это вопрос будет отражен в областях с другой юрисдикцией.

### Заключение

Мы движемся к обществу, которое становится все более зависимым от дистанционных транзакций, в которых участвуют как коммерческие, так и государственные организации. Вероятность мошенничества увеличиваются по ходу непрекращающихся изменений, выгодных преступникам и оказывающих негативное влияние на компании, которые легкомысленно относятся к предотвращению атак злоумышленников. В настоящее время уже существует инструментарий, позволяющий резко сократить преступления до небольшого и управляемого уровня. Соразмерное и строго в рамках закона их использование может изменить мнение преступников о том, что Интернет в настоящее время является для них землей обетованной.

*Перевод из журнала The Journal of Interactive Marketing. New Technology Briefing E-commerce and identity fraud Gareth Jones Vol. 2, No. 4, April/June 2001, p. 357-371. Печатается с разрешения издательства Henry Stewart Publications www.henrystewart.co.uk*

### Литература

Unpublished survey conducted by Experian in 2000; data drawn from @Internet Purchasing@ section, Nottingham.

Solomon v Soloman & Co. 1897 AC22 [Hl].

Experian (2000) Internet Fraud — A growing Threat to Online Retailers, Nottingham, Experain.

The Guardian (2000) 29 April.

Independent on Sunday (2000) 3 September.

Sunday Express (2000) 2 July.

Observer (2000) 20 August.

The Times (2000) 21 April.

Bristol Evening Post (2000) 18 August.

Experian ref. 3 above.

Ibid.

Scheer R. (2000) Nowhere to hide, Internt Life, October.