

50

**способов
отъема денег**

современного

Остапа БЕНДЕРА



50

способов
отъема денег
современного
Остапа БЕНДЕРА

МИНСК
СОВРЕМЕННЫЙ ЛИТЕРАТОР
2006

УДК 343.5
ББК 67.91
П 99

Автор-составитель Любовь СМИРНОВА

Охраняется законом об авторском праве. Воспроизведение всей книги или любой ее части запрещается без письменного разрешения издателя. Любые попытки нарушения закона будут преследоваться в судебном порядке.

П 99 50 способов отъёма денег современного Остапа Бендера / Авт.-сост. Л. Смирнова. — Мн.: Современный литератор, 2006. — 96 с.

ISBN 985-14-1155-8.

Волшебство на свете, может быть, и есть, но большинству людей с ним встречаться, вообще-то, не приходилось, разве что в цирке. А так хочется в него верить, особенно если оно приходит сразу да еще бесплатно. И этой беспредельной верой людей в чудеса ловко пользуются мошенники, и пределу их изобретательности нет конца.

Как избежать обычному человеку хитроумных ловушек, не попасть впросак, в силки жуликов, — об этом вы узнаете, прочитав эту очень поучительную книгу.

**УДК 343.5
ББК 67.91**

ISBN 985-14-1155-8

© Современный
литератор, 2005

ВВЕДЕНИЕ

...Ну вот. Опять обманули! И кричи не кричи теперь «милиция!». Ничего и никто не поможет...

И самое обидное — очень уж не хочется признаваться себе, что будь вы чуть-чуть сообразительнее... Чуть-чуть смекалистее... Да что там, попросту внимательнее! Однако что уже теперь говорить! Но на самом дне души царапает по-прежнему: ведь подсказывала же интуиция, что что-то не так, ведь очень хотелось с самого начала все это бросить!

Человеческое любопытство и человеческая небрежность — основные наши с вами качества, на которых играют, как правило, профессиональные мошенники. Согласитесь ведь, что не ради удовольствия поблизуствовать перед телекамерами, конечно, не ради умело брошенного в ответ ведущему красного словца стремятся наши с вами сограждане сделаться участниками телепередач «Поле чудес» и «Как стать миллионером». Но это, к счастью, занятия невинные, к тому же оборачивающиеся для многих ценным призом или, на худой конец, «памятным подарком».

К сожалению, в реальной жизни многим людям достаточно совсем немножко «повесить лапши на уши», как они готовы почувствовать себя путешественниками, отважно пересекающими поле чудес в поисках миллиона, которого просто не может не оказаться под тем вот ближайшим деревом.

И совсем неважно, что не вы, а кто-то другой уже пробормотал под нум «Крекс-фекс-пекс».

Как же не стать жертвой мошенников? К сожалению, часто нам приходится задавать этот вопрос себе «задним числом», в сослагательном наклонении, размышляя о том, как можно было бы не стать объектом изощренных махинаций «ловких» людей.

Эксперты правоохранительных органов не перестают удивляться — как легко ловятся на удочку авантюристов простаки. А ведь для того чтобы избежать их ловких сетей, несложно затвердить на память очень простые истины:

- ➡ если что-то звучит слишком заманчиво, чтобы быть правдой, — это неправда;
- ➡ реклама может обманывать. Не стоит всегда доверять рекламе;

- ➡ *внимательно читайте все пункты договора. Не подписывайте ничего, пока не убедитесь в том, что все положения соглашения понятны и устраивают вас. Требуйте объяснений, если вам что-то неясно;*
- ➡ *если некий пункт договора не зафиксирован в письменной форме, а обсуждался лишь на словах, это означает, что вас пытаются ввести в заблуждение;*
- ➡ *всегда узнавайте адрес, телефон и иные координаты компании, с которой вы вступили в контакт, и пытайтесь навестить о ней справки;*
- ➡ *не доверяйте фирмам, базирующимся не в вашем регионе;*
- ➡ *покупайте товары и услуги у компаний, которые находятся на вашей территории. В противном случае вы не имеете возможности заранее проверить их реальное качество;*
- ➡ *если вам делают коммерческие предложения по телефону, всегда требуйте предоставления полной информации в письменной форме;*
- ➡ *отказывайтесь от всех «конфиденциальных» предложений.*

Да, но что же делать, если вас все же обманули? Не сомневайтесь, у аферистов в 99 случаях из 100 отработан детальный план «реабилитации», и одними лишь методами самозащиты проблему вряд ли удастся решить.

Возможно, наши рекомендации покажутся вам наивными, однако очень многие преступления так и остаются нераскрытыми только потому, что иные граждане попросту не верят в эффективность поиска преступника по горячим следам, а еще чаще — просто впадают в транс, осознав, что стали жертвами «кидал».

Итак, если с вами все же случилась досадная неприятность, немедленно обращайтесь в милицию по месту совершения преступления. При этом надо иметь в виду, что в зависимости от характера совершенного в отношении вас правонарушения проверка может быть поручена как сотрудникам милиции общественной безопасности, так и оперативным работникам уголовного розыска или ОБЭП. При подаче заявления учтите, что любые детали, документы, показания свидетелей и других лиц могут облегчить поиск преступников. При наличии достаточных доказательств милиция работает гораздо оперативнее.

Да, возразите вы, но ведь часто по заявлениям об аферах выносятся постановления об отказе в возбуждении уголовного

дела с ссылкой на гражданско-правовые отношения и отсутствие состава преступления. Если вы все-таки считаете, что в отношении вас совершено именно преступление, постановление об отказе в возбуждении уголовного дела нужно обжаловать в прокуратуру.

А вот еще несколько советов и просто ценная информация.

1. В городах с населением свыше миллиона человек действует до 1,5 тысячи аферистов и воров; в городах от 500 тысяч до миллиона человек — 300. По подсчетам специалистов, в России ежегодно совершается до 15 миллионов краж; наказываемся же в лучшем случае десятая часть воров.

2. Если к вам подойдут на улице какие-либо граждане с просьбой, например, проверить, не фальшивые ли им «всучили» доллары, ничего не берите в руки: вы можете стать жертвой грубейшего шантажа.

3. Если ваш телефон неожиданно замолчал, виновата, скорее всего, не АТС, а жулики, воспользовавшиеся нелегальным подключением для передачи (приемки) криминальных сообщений. В этом случае необходимо немедленно связаться с АТС и потребовать проверить линию.

4. Для выяснения адресата телефонного шантажа незаменимы телефоны с определителем номера.

5. Ни один добросовестный продавец, как и покупатель, не будет скрывать свои данные. У партнера, который вам что-либо продает, необходимо выяснить и записать адрес, телефон, паспортные данные и лично убедиться в их подлинности. То же относится и к отдельным характеристикам реализуемой вещи, в том числе относящимся к ее качеству.

6. Постарайтесь ни при каких условиях не передавать деньги, даже на ограниченный промежуток времени, до окончательного оформления права собственности или реальной передачи вам вещи.

7. Существует масса способов обеспечить исполнение обязательств (залог, задаток, удержание, поручительство и пр.), которые необходимо использовать с умом.

8. Никогда ни при каких обстоятельствах не перечисляйте по почте деньги на «зазывные» объявления (об учебе, работе, туристской и прочей поездке, лечении и т. п.), когда указаны лишь почтовый ящик (п/я) или расчетный счет (р/с) получателя, но не его адрес. Так или иначе, но вас обязательно обманут.

Часто речь идет о коллективном обмане — мошенничестве против группы лиц, объединенных общими интересами.

Многие преступники в целях завоевания доверия своих будущих жертв используют их религиозную, этническую, возрастную, профессиональную или другую общность, зная о характерной особенности человеческой природы доверять тому, кто на тебя похож. Организаторы мошенничества часто сами являются членами общины или только заявляют о своей принадлежности к ней, ссылаясь на ее авторитетных и уважаемых членов. Злоумышленники цинично делают ставку на доверие и дружбу, складывающиеся в коллективе людей, которых связывает что-то общее. Этот прием срабатывает.

Представители российских правоохранительных органов говорят, что коллективные обманы особенно сложно выявлять, учитывая тесные связи и закрытость большинства групп и естественное нежелание с их стороны «выносить сор из избы».

Жертвы подобных афер часто предпочитают не прибегать к помощи властей и законным методам преследования, а самостоятельно разбираются с проблемой внутри общины или группы.

Казалось бы, все советы давно вам известны. Однако чего только стоит старый хорошо известный, но вместе с тем до сих пор удачно действующий способ, который часто используют мошенники! Заключается он в следующем. Идет себе человек спокойно по улице, как вдруг подходит к нему прохожий и спрашивает: «Извините, я тут кошелек нашел, это случайно не Вы потеряли?» Естественно, что после проверки наличия собственного кошелька звучит отрицательный ответ. Тогда новый знакомый открывает найденный кошелек и с радостью обнаруживает в нем крупную сумму денег. В порыве радости он предлагает новоиспеченному знакомому отойти в безлюдное место, подальше от любопытных взглядов, и поделить найденное поровну. Надо сказать, что в такой ситуации у большинства людей робкий голос совести легко заглушается воплем жадности. Еще бы, такая удача, деньги сами плывут в руки, когда еще так пощастливится. Но поделить деньги так и не удастся. В самый неподходящий момент появляется хозяин кошелька, причем иногда в компании с грузьями. Естественно, что за этим следует требование вернуть утерянное. Далее все может развиваться по нескольким сценариям. По одному из них жертву обвинят в краже и потребуют отдать

деньги, которые были в кошельке. В ответ на оправдания и заверения в том, что он никаких денег не брал, предложат продемонстрировать содержание кошелька, в котором наверняка лежат украденные деньги. Деньги тщательно пересчитают и, удостоверившись, что в кошельке нужной суммы нет, настоятельно попросят показать содержимое карманов или сумки. Обычно попавший в подобную ситуацию человек редко бывает против, и даже сам активно старается доказать собственную невиновность. В общем, скандал на повышенных тонах будет продолжаться некоторое время, пока неудачнику не предложат удалиться. Между тем в ходе «активного разбирательства» мошенники успевают продемонстрировать ловкость рук и, как правило, деньги и ценные вещи жертвы перемещаются в их карман. Естественно, что жертва, занятая объяснениями, этого не замечает и спешит поскорее удалиться с места конфликта, радуясь, что все так благополучно закончилось. Пропажа будет обнаружена намного позже, причем далеко не всегда она связывается с этим неприятным инцидентом. Гораздо чаще люди думают, что деньги и вещи украли в транспорте, или предполагают, что они их просто где-то потеряли.

ГЛАВА 1

КИРПИЧ, КАК ИЗВЕСТНО, НИКОГДА НИ С ТОГО НИ С СЕГО НА ГОЛОВУ НЕ ПАДАЕТ

Кому из нас не попадались на глаза объявления следующего содержания. «Работа на дому, пять видов. Возможна частичная и полная занятость. Обработка и рассылка корреспонденции. Заработок до 400 долларов в месяц».

«10 видов надомной работы... Рассылка почты и деловой корреспонденции. Заработок до 150 долларов в неделю. Ответим всем».

«Нужны люди для обработки корреспонденции на дому. Рассылка полуфабрикатов и карточек. Занятость 2—4 часа в день, з/п от 1000 долларов».

И таких объявлений можно найти по десятку в каждом более или менее престижном печатном издании. От обещаемых сумм заработка просто сердце замирает. «А вдруг что-то стоящее?» Ведь написано во многих объявлениях: «Ваш доход зависит от вашей личной работоспособности и инициативы»...

1. ОПЛАТА БУДУЩЕГО «ТРУДОУСТРОЙСТВА»

Ответы от фирм, которым вы решитесь написать, придут на удивление быстро. Чаще фирмы, по утверждению их менеджеров, занимаются «социальными программами, которые помогают людям найти высокооплачиваемую работу на дому, не требующую ни специальных знаний, ни начального капитала и занимающую минимум времени». Однако информаторы мягко предупредят: «Просто так деньги не даются никому. Ваш достаток — это ваше желание и трудолюбие». Тем не менее стабильный доход до 7—8 тысяч долларов в год вам гарантируют.

Для получения более конкретной информации нужно оплатить почтовым переводом одноразовый взнос. Этот взнос, обычно говорится, необходим для подготовки и распечатки документов по выбранному вами виду работ, а также как средст-

во защиты «от тех, кто относится к нашей работе несерьезно». Чтобы развеять последние сомнения, в информации значится многообещающее: «Все предлагаемые работы юридически законны. Мы не имеем ничего общего с деятельностью организаций и частных лиц, злоупотребляющих доверием людей в корыстных целях и для проведения каких-либо мошеннических операций».

Наверное, здесь бы вам и остановиться. Если для поступления на работу требуют оплату, к тому же почтовым переводом на абонентский ящик, — это уже явный «кид-няк», но... Что же все-таки дальше-то?

Переводите вы «фирме» требуемые денежки. Не такие уж и большие, кстати. Дней через десять получаете «Программу почтовой работы». В ней говорится, что первый шаг к своей финансовой независимости вами сделан, что программа эта — просто спасение от безденежья в эпоху тотальной безработицы и все теперь зависит лишь от вашего трудолюбия.

В первой рекомендации значится следующее: «Для наиболее успешной работы и максимальной от нее отдачи необходимо пройти регистрацию и получить базовую информацию по остальным видам работ». Словом, предлагается снова платить за рассказы о других работах и снова платить за внесение сведений о вашей личности в банк данных. Отдельная плата требуется за уведомление о новых видах высокодоходных работ. Дело поставлено хитро: заплатив все эти суммы, здравомыслящий человек уже не сможет остановиться на полпути, а будет платить и платить, все еще надеясь на чудесный результат.

Сама «Программа почтовой работы» составляется, очевидно, весьма неглупым человеком, но за всеми грамотно и красиво сформулированными фразами сквозит одна мысль: теперь вы сами должны «ловить на удочку» доверчивых простаков, помещая объявления в газетах и расклеивая их на столбах, рассылая информационные листки от имени фирмы, но уже со своими данными. «Работодатели» даже предлагают помощь (не бесплатную, естественно) в создании «исходной» формы европейского уровня и лазерного качества для дальнейшего «классного ксерокопирования».

Рекомендации, как подыскивать дурачков, вообще уникальны. Есть смысл привести их полностью. Скажу только, что весь упор тут делается на рекламу: «...если у вас есть хоть

небольшие финансовые возможности, мы рекомендуем вам подавать объявления в платные рекламные издания... Платная реклама публикуется в течение пяти дней, в то время как бесплатная — в течение месяца. Чем шире будет сеть вашей рекламы, тем больше откликов вы соберете... Важно знать, как сделать ваше объявление привлекательным. Используйте слова: «Вы можете прилично заработать!», «Невероятно высокий доход!», «1000 долларов в неделю!». Но будьте корректны. Помните, что ваш будущий клиент должен вам верить. Цену назначайте умеренную — шанс получить больше заказов. Через некоторое время к вам будут приходить отклики. Количество заявок, по среднестатистическим подсчетам, достигает 600—800 писем в месяц. В полученный подписанный конверт клиента вы вкладываете свой информ-листок. Затем к вам будут приходить ответы-запросы с квитанциями почтовых переводов и подписанным конвертом. Вы вкладываете заказную инструкцию и отправляете ее клиенту. С точки зрения закона, вы являетесь продавцом информации, а это ненаказуемо». И еще приписка: «С нашей стороны все условия выполнены. Вы хотели иметь на дому самостоятельную доходную работу и получили соответствующие инструкции... Желаем удачи!»

Лет шесть назад в моде был такой ловкий ход. Кто-то давал объявление в газету: «Научу, как в месяц заработать до 100 миллионов. От вас конверт с обратным адресом и квитанция о переводе...». Далее указывался номер счета и небольшая сумма — тысяч 200—300 (тогда мы еще все были «миллионщиками»).

Клюнув на эту наживку, вы через неделю получали ответ: «Хотите хорошо зарабатывать? Дайте в газету аналогичное объявление». Ничего не скажешь. Растет интеллектуальный уровень мошенников.

2. БАБЕТТА ИДЕТ НА «СОБЕСЕДОВАНИЕ»

А вот «крутой» вариант. Вы приходите в красивый офис, начиненный современной оргтехникой. С вами проводят предварительное собеседование, сулят вам зарплату (не менее 500 долларов) и ставят неременное условие — дома должен быть факс, компьютер, ксерокс и т. д. Естественно, мало

у кого дома есть весь этот набор. Тогда вам предлагают выкупить у офиса необходимую оргтехнику, а точнее, дать деньги — небольшие, очень небольшие в сравнении с тем, сколько эта техника, новая или даже подержанная, стоит в компьютерном салоне или в комиссионном магазине. Вы закупаете «железо», потратившись, разумеется, на его перевоз, и далее ждете обещанного сотрудника, который вам все подключит и научит пользоваться, а заодно и выдаст первое задание.

Итак, вы все это приобретаете, вас обещают загрузить работой, вы ждете — надо же им набрать еще «сотрудников» для нормальной работы, — и, разумеется, через определенное время вы понимаете, что никто вам больше не позвонит, деньги ушли, а вы остались, как объяснит вам толковый специалист, с полуживой оргтехникой, на которой работать, в общем-то, нельзя.

3. КУРСЫ ДЛЯ ЖЕЛАЮЩИХ «НАЧАТЬ НОВУЮ ЖИЗНЬ»

Знакомая ситуация — вы решили сменить работу. Например, декретный отпуск закончился, возвращаться в прежний институт не хочется. Или, наоборот, вы мужественно закончили заочное отделение гуманитарного факультета и, наконец, решились расстаться с местом высокооплачиваемой швеи в престижном салоне вечернего платья. Но так хочется начать новую жизнь, почувствовать себя работником умственного труда! И вот — объявление! Да такое, что сразу видно — никакого мошенничества.

Популярный телеканал объявляет о том, что на его базе создаются курсы для будущих телеведущих. Требований всего два — интересные внешние данные, возраст до 35 лет и сумма в размере 300 долларов, которую необходимо заплатить на четыре месяца обучения. А потом — трудоустройство на этот самый канал. Разумеется, не всех, а лучших.

Возможно, уже в первый день занятий вас не оставляет в покое неприятная мысль — всего курсантов около сорока, а трудоустроят, как подсказывает здоровая логика, от силы человек пять. Но поздно, деньги уже уплачены, да и учеба начинается — ежевечерняя, изматывающая, но очень интересная.

Вам преподают разнообразнейшие предметы — стиль, искусство визажа, декламацию, учат владеть жестами, «говорить глазами»... Попутно для вас проводят «мастер-классы» популярнейшие телеведущие, которых прежде вы видели лишь на телеэкране. На мастер-классах они рассказывают вам забавные истории из своей жизни. Потом начинаются практические занятия — съемки. Видеокассеты, естественно, заполнены не целиком, и на оставшиеся места ваш руководитель снимает вас, проводя бесконечные кастинги вашего умения выразительно рассказывать о прогнозе погоды и шутить в эфире.

Курсы заканчиваются, и вы узнаете, что из вашей группы в «счастливчики» никто не попал. Оказывается, позже будут занятия еще с двумя группами, возможно, настоящие «звезды» именно там. А у вас пока на всякий случай возьмут телефон.

4. ХОТИТЕ НАУЧИТЬСЯ БРИТЬ ПОДМЫШКИ?

Эта и подобные «услуги» ориентированы, в первую очередь, на людей ленивых, нелюбопытных и очень не любящих толкаться по магазинам, салонам, а также выяснять у подружек, что в каком из них продают.

Представьте, что вы видите объявление в недорогом женском журнальчике: «Не нужно мучиться с ежедневной депиляцией! Не нужно плакать в ванной, пытаясь справиться с растительностью, произрастающей в самых неподходящих местах!» Далее сообщается о том, что вы можете получить чудодейственное средство химического содержания (то есть ничего брить не нужно, достаточно нанести на кожу некую мазь или крем), если отправите заказ на него по указанному абонентскому ящику вместе с почтовым переводом.

Некоторое время спустя вы получаете извещение о том, что наложенным платежом на почту для вас поступил пакет. Разумеется, это обещанное косметическое средство! Вы направляетесь в свое отделение связи, рассчитывая получить сверток, но вместо него видите обычный почтовый конверт.

Да, но не ругаться же при почтальонах, не требовать же при них вскрытия — та ли это мазь, которой вы собираетесь удалять волосы под мышками!

Дома вы вскрываете конверт и видите распечатку или ксерокопию, на которой перечисляются пять-шесть способов приготовления некоего снадобья в домашних условиях. И если вы человек без чувства юмора и попытаетесь приготовить то, что вам предлагают, и даже натереть этим «чудодейственным» средством кожу, то через какое-то время она покроется язвами и вам понадобится дерматолог и больничный.

5. КУПИТЕ ОТКРЫТКУ ДЛЯ ДЕТЕЙ-СИРОТ

Это весьма распространенный вид мошенничества, которым не брезгуют студенты, старшие школьники и просто молодые люди, которые не видят особого греха в том, чтобы выудить у вас пару рублей. Главное — молодые люди при этом должны хорошо выглядеть и производить впечатление «детей из хороших семей».

К вам подходят две миловидные девушки, представляются членами студенческого благотворительного объединения «Жар-Птица» или «Семеро козлят», на что фантазии хватит. Они рассказывают вам, что участвуют в опеке какого-нибудь приюта или детского дома и собирают средства в помощь детишкам путем продажи открыток.

В руках девушек появляется большой альбом с открытками — виды городов, растения, птицы, зверюшки. Мелодичными, усыпляющими голосами девушки говорят вам о том, что можно приобрести любую понравившуюся вам открытку за любую сумму, которую вы готовы пожертвовать на помощь сиротам.

Во-первых, срабатывает психологический эффект — девушки не кланчат деньги, а предлагают вам сделать покупку, пусть и символически-трогательную. Именно это ощущение трогательности и побуждает вас расстегнуть кошелек. И, разумеется, вы уплатите за открытку не символическую копейку, а еще, вероятно, и открытку выбирать не станете, просто дадите девушкам денег.

И вряд ли вы задумаетесь о том — неужто действительно продажей открыток можно собрать столько денег, чтобы улучшить материальное положение сирот? Вот материальное положение двух девушек, которым до зарезу понадобились деньги, — да, запросто.

6. ОБОРУДОВАНИЕ ДЛЯ ПРОСМОТРА КАБЕЛЬНОГО ТЕЛЕВИДЕНИЯ

Большинство людей любят приобрести что-либо по дешевке. Особенно, если дешевые расценки касаются «дорогих» бытовых услуг.

За небольшую сумму вам предложат купить устройство для подключения к сети кабельного телевидения (естественно, без ведома администрации сети). Фокус в том, что большинство из них работать не будет. Более того, вас могут обнаружить — и простым предупреждением отделаться будет очень трудно.

7. ЛОТЕРЕЙНЫЙ «ЛОХОТРОН»

О том, что многочисленные лотереи, столь популярные на рынках, во всех людных местах не что иное, как обман, знают и догадываются, пожалуй, все. Но почему-то упорно продолжают пытаться счастья в наивной надежде, что им все-таки повезет. Казалось бы, сколько уже говорили о том, что игра «в наперстки» — это не более чем спектакль, поставленный с целью облапошить человека, желающего подарить свои деньги. И давно известно, что угадать, где шарик, все равно не удастся, — просто потому, что шарика под наперстками нет — ловкие «каты» зажимают его между пальцами. Старо и банально, а все равно нет, нет, да и попадется еще один азартный игрок.

Правда, последнее время подобные способы уже уходят в прошлое; народ, наученный горьким опытом, на удочку к мошенникам не попадает. Но ведь они, мошенники, тоже на месте не стоят и придумывают новые, более изощренные способы. Например, наиболее популярным сейчас является «выигрыш в лотерею».

Происходит это следующим образом. К человеку подходит приятного вида, аккуратно одетый, вежливый юноша (или девушка) и сообщает, что он (или она) является представителем фирмы «Х», которая проводит беспроигрышную, бесплатную лотерею. В случае, если намеченная жертва заинтересовалась, ей предлагают вытянуть билетик (иногда сразу объявляют о выигрыше). Счастливцу тут же сообщают, что приз (телевизор,

магнитофон или иная ценная вещь) ждет его. Но тут неожиданно выясняется досадное недоразумение — на этот приз претендует еще один человек. Чтобы никого не обидеть, предлагается провести своеобразный аукцион. Кто больше денег поставит, тому и приз достанется. Движимый жаждой азарта — еще бы, вот же он приз, — человек начинает делать ставки, передавая организаторам энные суммы из своего кошелька. Но, как ни странно, его соперник всегда ставит чуть больше.

Для тех, кто еще не понял, поясняем: претендент на приз — это сообщник мошенников. Когда деньги заканчиваются, организаторы предлагают съездить за деньгами домой и даже соглашаются подвезти на своей машине.

Далее следует поездка домой и новая, на этот раз уже значительная сумма. Казалось бы, победа уже близка, но, увы, второй участник все-таки перекрывает ставку большей суммой и забирает приз. А несчастному проигравшему предлагают не расстраиваться и уверяют, что ему повезет в другой раз. Но самое интересное — все его ставки остаются у мошенников, которые быстро ретируются.

Жертвами мошенничества нередко становятся люди умные и здравомыслящие. А все дело в том, что мошенники зачастую талантливы и обладают хорошими познаниями в психологии. Сам процесс розыгрыша проходит виртуозно и на таком эмоциональном всплеске, что разум жертвы просто затуманивается. Есть также обоснованные подозрения, что в подобных случаях используются гипноз и манипуляции сознанием.

Для того чтобы не попадать в подобные ситуации, никогда не принимайте на улице предложений сыграть в лотерею. Если вам сообщают, что вы якобы выиграли приз, — откажитесь. Помните, бесплатный сыр бывает только в мышеловке.

8. «ЖАДНОСТЬ ФРАЕРА СГУБИЛА»

Чтобы не попасть на удочку мошенников, важно всегда и внимательно читать текст, написанный мелким шрифтом. Вот конкретная ситуация. Вы получаете по почте красиво оформленный лотерейный билет. Билет, судя по тому, что на нем написано, бесплатный. Нужно лишь стереть серебристую краску с находящегося в центре квадрата и посмотреть,

не «выпадут» ли три крестика или три нолика подряд. Если выпадут — кричите «ура», ведь вы почти что выиграли аж 10 000 долларов. Разумеется, раз лотерея бесплатная, то грех не попытаться счастья. Итак, стирая серебряную краску, вы обнаруживаете под ней выигрышную позицию — три крестика по диагонали.

Стало быть, 10 000 долларов почти что ваши. Как же теперь получить эти самые 10 000? Этого на билете не указано, а пропечатан только номер телефона, по которому вам и предложено позвонить.

Считая, что заветные 10 000 у вас в кармане, вы хватаете трубку телефона, набираете номер и... вот неудача! У вас на билете номер 101-202-303, а выиграл билет номер 101-202-304. Ну да ладно — Бог дал, Бог взял. Вы вешаете трубку, рвете билет и забываете об этом случае. Увы, забываете ненадолго.

Через некоторое время к вам приходит счет за телефон, который почему-то долларов этак на 20 больше обычного. В чем дело? Да тот номер, по которому вы звонили, начинался на 1-900. Или же был из серии 1-888-239-1384. И звонок по этому нехорошему номеру стоит 20 долларов (плюс 3 доллара налогов), даже если вы говорили всего лишь 30 секунд.

Да, но на каждом билете, помимо броских рекламных надписей, было очень мелким шрифтом напечатано, что «Звонок стоит 20 долларов + налоги», что «Всего будет распространено 10 миллионов билетов, из коих выиграет только один», что «Возможность» выигрыша — еще не сам выигрыш».

В пылу золотой лихорадки эти примечания мало кто удосужился прочесть.

И еще один пример самой настоящей денежной лихорадки. В один прекрасный день несколько сот тысяч человек получили по почте ярко раскрашенные конверты. В конверте был образец чека на 2500 долларов и письмо, из коего следовало, что сам чек будет выслан тому, кто пошлет 10 долларов организаторам — какому-то обществу. Но не каждому, а только тому, чьи 10 долларов будут получены обществом раньше остальных.

Заманчиво? Еще бы. Ведь есть же реальная возможность быть первым и получить этот чек на две с половиной тысячи! Конечно, если вы пошлете деньги обычной почтой, то вы наверняка проиграете; но ведь можно же послать конверт и курьерской почтой — уж тогда-то он точно придет самым первым!

И бросились десятки тысяч людей на почту — отправлять пакеты да переводы... А кто же все-таки был первым? Кто выиграл в этой сказочной лотерее? Этого не знает никто. Весьма вероятно, что первым пришел конверт одного из участников этой аферы или какого-нибудь подставного лица. Но даже если и нет, то все равно не беда — за несколько дней «денежной лихорадки» господа «предприниматели» собрали гораздо больше, чем 2500 долларов.

ГЛАВА 2

«МОБИЛКИ» ДЛЯ ЛОХОВ, или КАК ТЕЛЕФОН В РУКАХ ПРЕВРАЩАЕТ ЧЕЛОВЕКА В ОБЕЗЬЯНУ

9. «ДЕТИ ЛЕЙТЕНАНТА ШМИДТА»

На телефон абонента поступает звонок. Звонивший представляется сыном (братом, другом, сослуживцем) абонента и взволнованным голосом сообщал, что только что он попал в аварию (сбил человека, задержан милицией, взят в заложники, застрял в лифте). Непривычное звучание голоса объяснял стрессовым состоянием, травмой, плохой связью. Почему звонок с чужого телефона? У моего сели батарейки (сломался во время аварии, отобран бандитами, потерялся в суматохе) — приходится звонить с чужого. Звонить придется много, поэтому надо пополнить человеку баланс. Далее следовала просьба купить карточку экспресс-оплаты на 10, 20, 50 и даже 100 долларов и продиктовать по телефону ее секретный код.

В такой ситуации мошенники демонстрируют хорошие знания психологии. Они делали все, чтобы не дать «клиенту» выйти из стрессовой ситуации, понимая, что способность здраво мыслить в состоянии шока притупляется.

По ходу злоумышленники стараются выяснить как можно больше о личной жизни жертвы — имена родственников, место проживания, все, чтобы не дать ей усомниться в том, что мошенник — именно тот, за кого себя выдает.

По всей видимости, первые несколько месяцев злоумышленники ограничиваются тем, что пополняют баланс своих мобильных телефонов. Но потом система мошенничества приобретает более серьезный характер. Теперь злоумышленники просят своих «родственников» не только пополнить баланс, но и умудряются раскручивать их на наличные деньги. После пополнения баланса следует еще один звонок. Мнимый родственник облегченно вздыхает и сообщает своим «родственникам», что конфликт удалось уладить полюбовно — от пострадавших в ДТП (милиционеров, бандитов) удалось откупиться. Нужно лишь в условленном месте передать посредникам деньги. Далее называется сумма от 300 до 1500 долларов.

10. КЛОНИРОВАНИЕ ТЕРМИНАЛОВ

Наиболее известным типом мошенничества в сотовой телефонии является клонирование терминалов, особенно распространенное в сетях аналоговых стандартов. Этим термином обозначают программирование параметров легально зарегистрированного сотового аппарата на другом терминале.

Известны случаи, когда для одного телефона было создано сразу несколько клонированных копий. Надо ли объяснять, что счета за разговоры с клонированного телефона придется оплачивать владельцу трубки-прототипа.

Параметры, необходимые для программирования, обычно добываются в ходе прослушивания эфира, через который сотовый телефон и базовая станция обмениваются служебной информацией, либо путем простой кражи. (Кстати, кража самих терминалов, несмотря на дешевизну многих моделей, по-прежнему широко распространена, в том числе из-за возможности сделать множество дорогостоящих звонков, прежде чем оператор заблокирует счет, «привязанный» к украденному аппарату.)

Получатель счетов с явно завышенными суммами редко остается безучастным к происходящему, так что его аппарат получает у оператора новый идентификатор, а старые данные блокируются. Чтобы обойти это препятствие, злоумышленники используют технологию «кувыркания» (tumbling) — вариант клонирования, при котором в телефон-копию закладываются идентификаторы сразу нескольких (они могут исчисляться

десятками) аппаратов-прототипов; при осуществлении вызова они выбираются поочередно. Указанная модификация уменьшает вероятность обнаружения клонированного телефона в сети и продлевает срок его службы до того момента, когда будет заблокирован последний из исходных идентификаторов. Телефоны, клонированные по методу tumbling, часто продаются на «сером» рынке с гарантией работоспособности в течение определенного срока; если трубка окажется заблокированной раньше, поставщик произведет бесплатную замену.

Согласно имеющимся оценкам, в США ежемесячно клонируются около 75 тысяч телефонов, и, судя по всему, эта проблема исчезнет лишь тогда, когда аналоговые сотовые сети окончательно уйдут со сцены.

В ряду проделок мошенников, специализирующихся на мобильной связи, существенный вес имеют махинации с услугами роуминга. Здесь, как и при дальней связи в фиксированной телефонии, используется временной лаг, возникающий между моментом активации функции роуминга и тем временем, когда операторы уже обменялись биллинговой информацией. Наконец, множество схем мошенничества разработано для сотовых сетей с предоплатой

Возможность не заботиться о кредитной истории клиента и его текущей платежеспособности стимулирует повышенный интерес операторов к предоставлению услуг сотовой связи с предоплатой. Более того, оплата услуг с помощью телефонных карт избавляет операторов от процедур выставления счетов и контроля за их своевременной оплатой, а ведь не секрет, что биллинговые системы очень сложны в эксплуатации и довольно часто дают сбои.

Многие операторы считают продажу телефонных карт весьма эффективным способом привлечения новых клиентов, который к тому же снижает риск телефонного мошенничества.

К сожалению, последний тезис имеет мало общего с действительностью. Практически ничего не зная об абонентах, которые приобретают телефонные карты в самых разных местах, оператор открывает свою сеть для мошенников всех мастей. Не располагая многофункциональной биллинговой системой и надежными средствами администрирования, такой оператор зачастую даже не догадывается, каковы истинные масштабы ущерба, причиненного злоумышленниками. А его

размеры составляют 3—5 % суммарного дохода оператора, причем методы мошенничества учитывают специфику услуг с предоплатой.

Наиболее уязвимым местом является сама телефонная карта, а точнее, содержащийся на ней скрытый цифровой код. Нередки ситуации, когда этот код становится известен мошенникам еще до продажи карты, и ничего не подозревающий покупатель с удивлением обнаруживает, что бюджет только что приобретенной карты уже исчерпан. Украденные коды воспроизводятся на поддельных картах.

Что касается методов получения секретного кода, они на удивление просты. В одних случаях код просто может быть прочитан сквозь целлофановую упаковку, в других эту упаковку можно вскрыть, а потом запечатать. Профессионалам удается даже стереть защитный слой на поле секретного кода, а затем восстановить его.

Невольными сообщниками мошенников нередко становятся сами изготовители телефонных карт. Секретные коды бывают неоправданно короткими, поэтому их без труда могут запоминать сотрудники, работающие на конвейере. Кроме того, им порой удается скопировать секретную информацию или попросту украсть ее для последующей продажи. Известен случай, когда якобы из-за сбоя печатающего устройства для большой партии карт были изготовлены двойники, содержавшие те же секретные коды. Карты-двойники поступили в розничную сеть наряду с оригиналами, и совокупный ущерб от этой «ошибки принтера» превысил 1 миллион долларов.

Очень часто производитель рассматривает только что изготовленные карты как обычную печатную продукцию и не принимает специальных мер для обеспечения их безопасности при хранении и транспортировке. На деле же телефонные карты являются эквивалентом наличных денег (отличие заключается в том, что карты не могут служить средством платежа многократно).

Другой объект пристального внимания мошенников — средства управления счетами абонентов. Если говорить о сетях стандарта GSM, то на сегодняшний день наиболее уязвимы решения, предусматривающие хранение финансовых сведений непосредственно в SIM-карте. Эта информация в принципе может быть изменена извне. К счастью, такое изменение

всякий раз затрагивает только одну карту, и случаи клонирования SIM-карт пока не известны.

11. БЕСПЛАТНЫЕ ТЕЛЕФОННЫЕ ЗВОНКИ ОТ ОПЕРАТОРА «ЛОХ-GSM»

Тотальная телефонная мобилизация нашего населения и пока еще высокие тарифы на сотовую связь не могли не породить еще один новый вид мошенничества. Догадываетесь? Конечно, они самые, обещания золотых гор в виде возможности бесплатных исходящих звонков.

Поднимите руки те, кто не получал по электронной почте сообщений типа:

«Здравствуйте. Сколько Вы платите за звонки по сотовому телефону? У Вас есть возможность сделать бесплатными исходящие звонки и SMS-сообщения — мы Вам ее предоставим. В результате Вы можете получить анонимный, непеленгуемый телефон с возможностью неограниченных исходящих звонков».

Не сомневайтесь, что у владельца «трубки», впервые обнаружившего в своем почтовом ящике подобный текст, тут же возникнет желание подробнее ознакомиться с предложением и зайти на указанный сайт (стремление к «даровым» услугам в нашем народе — элемент национального менталитета). Адресов, где располагаются многочисленные клоны сайтов, предлагающих, естественно, не безвозмездно, программку, якобы позволяющую избежать расходов на оплату исходящих звонков и SMS-сообщение, огромное множество.

На титульных страницах всех «бесплатных GSM-щиков» опубликован стандартный текст, стилизованный под искренний и откровенный рассказ разработчика о том, как он, ведомый благородными чувствами и лютой ненавистью к живодерам-операторам, придумал эту самую программку и готов с радостью (как становится ясно, для себя самого) поделиться ею с пользователями. И цена вроде невелика — «прошивка» (программа) для одного телефона стоит 50 долларов. Кроме того, существуют оптовые скидки...

Если взять за критерий количество сайтов, на которых появляется то или иное предложение, то номером один является афера, в которой жертвам предлагается купить «прошивку» для мобильного, позволяющую якобы говорить по телефону бесплатно.

Текст на всех этих сайтах один и тот же, хотя делают их разные люди — просто копируют содержание с первого такого сайта, который появился в сети года два назад.

Афера продумана очень грамотно: наукообразный текст, список операторов мобильной связи, с которыми «прошивки» работают, перечень мобильных телефонов и т. д. Приводимое обоснование возможности бесплатной связи — полная чушь, но на всех это действует.

Если вы попросите по e-mail сообщить вам электронные адреса тех, кто уже пользовался этой услугой, вам их предоставят, но адреса будут, разумеется, подставными. Жертва переводит на счет такого афериста деньги — и не получает в ответ вообще ничего.

Варианты мошенничества, связанные с мобильной связью, не ограничены многочисленными проектами Free GSM. Вы можете столкнуться в Интернете с проектом «GSM-пират», где вам предложат модернизировать телефон так, что вы сможете разговаривать за счет других абонентов. Или натолкнуться на сайт, где вам предложат купить программу, генерирующую Pin-код для пополнения счета, например cardgennew.narod.ru. Последняя новинка в области интернет-афер, связанных с мобильными телефонами, — сайт sms-revolution.narod.ru. На этом сайте рассказывается об «уникальной возможности» получить неограниченный доступ к отправке SMS-сообщений с телефона благодаря тому, что авторами сайта реализован свой центр по отправке SMS. Все это аферы чистой воды.

Еще одним вариантом аферы является дешевый доступ в Интернет.

Например, по адресу livejournal.com/users/kippie/592988.html № cutid1 находится описание программы, которая якобы позволяет полноценно пользоваться Интернетом через бесплатный гостевой вход, как правило, предоставляющий своим пользователям крупные провайдеры (под гостевым входом имеется в виду возможность бесплатно походить по сайту самого провайдера). Программа стоит \$ 8 и является 100 %-ным надувательством: пользоваться Интернетом через гостевой вход невозможно. В случае с moscow.ru речь может идти о торговле ворованными паролями доступа в Интернет, но, скорее всего, это обычное «кидалово», такое же как в случае с Free GSM: вы переводите деньги и ничего не получаете взамен.

12. МОШЕННИЧЕСТВА С ТЕЛЕФОННЫМИ КАРТАМИ

Хитроумные обманщики на этот раз действуют следующим образом: после вашего звонка по уличному таксофону к вам подходит симпатичная девушка и просит воспользоваться вашей телефонной карточкой в обмен на рубль или полтора.

После короткого звонка девушка действительно возвращает вам карту и рубль. Однако при следующей попытке воспользоваться карточкой, скорее всего, обнаружится, что на ней нет ни одной кредитной единицы.

Новые мошенники действуют просто: поскольку картинки на наиболее ходовых телефонных картах одинаковы, после звонка вам возвращается точно такая же карта, но «пустая». Самое любопытное, что обман в большинстве случаев сразу не раскрывается — обе карты отличаются друг от друга только серийными номерами, которые владельцы карт вряд ли запоминают.

Есть несколько средств спасения от надувательства. Во-первых, можно потренировать свою память, запомнив десять цифр серийного номера своей карточки. Для людей ленивых и имеющих проблемы с памятью можно порекомендовать просто пометить карту ручкой или фломастером. Как говорят очевидцы, такое нехитрое действие весьма успешно отпугивает мошенников.

Еще один вид «творчества» мошенников — подделка телефонных карт. Вооружившись заточенным до остроты иголки паяльником, «умельцы» перекраивали микросхему самой дешевой телефонной карты так, что таксофон мог определить наличие тарифных единиц, но не мог их изменить в памяти.

При использовании телефонной карты находящаяся на ней информация об отсутствии тарифных единиц не поступала в телефонный аппарат, что позволило пользоваться услугами связи без оплаты.

13. МГНОВЕННАЯ УСТАНОВКА ДОМАШНИХ ТЕЛЕФОНОВ

Телефонизация районов-новостроек сейчас идет сравнительно быстро. Если уж очень надо, то с доплатой можно поставить аппарат за считанные дни. Вот в эту нишу и вклинились мошенники.

«Благодетели» от имени телефонного узла предлагают мгновенную установку телефона, разумеется, за двойную-тройную цену. И что удивительно, не требуют деньги вперед, а действительно ставят работающий аппарат. И тут же предлагают опробовать. Сделав короткий радостный звонок родственникам, жилец так же радостно расстаётся с деньгами и получает на руки квитанцию и заветный номер.

Разочарование приходит иногда через час, иногда через день, когда телефон на все попытки дозвониться отзывается сигналом «ту-ту-ту-ту...». Часто жилец просто становится постоянным невольным слушателем чужих разговоров (о чем, кстати, иногда ничуть не жалеет).

Делается все довольно просто. Мошенники вычисляют первых обладателей телефонов в доме-новостройке. Потом спаривают номер с ними. Либо еще проще — ставят вам телефон как трубку-отводку. Момент для мгновенной постановки выбирают, когда истинного владельца номера нет дома и его телефон свободен для пробного звонка. За это время телефонные дельцы успевают в одном и том же доме прокрутить сразу несколько сделок и благополучно скрыться.

Или вот еще одна ситуация, исходя из которой вы можете оказаться в ловушке «телефонных» мошенников. Как это делают? Приходят к вам домой, например, и, представившись работником соответствующей организации, говорят: «Поздравляем, подошла ваша очередь на телефон, нужно подписать договор и оплатить первый взнос». Человек обрадован — какой сервис: не надо никуда идти, да и представитель внушает доверие (одет хорошо и выглядит прилично, по-деловому).

Само собой, «первый взнос» уходит в руки мошенников, а жертва снова собирает деньги на настоящий первый взнос.

ГЛАВА 3

КВАРТИРНЫЙ ВОПРОС, КОТОРЫЙ ЗДОРОВО ИСПОРТИЛ ЖИЗНЬ МНОГИМ ЛЮДЯМ

Скажите, часто ли вы на улице обращаете внимание на так называемых бомжей? А часто ли вы задумываетесь о том, как

они стали влечать столь жалкое существование? Или вы искренне верите в то, что все они — жертвы собственной распущенности и злоупотребления спиртным?

Самое дорогое имущество, которое имеется у большинства наших сограждан, — это квартира. Потому и не удивительно, что сфера продаж квартир стала сегодня весьма криминализированным бизнесом.

14. «НЕХОРОШАЯ» КВАРТИРА

Самая примитивная мошенническая сделка по продаже недвижимости — это продажа чужой квартиры. Документы на квартиру могут быть либо подделаны, либо изготовлены с использованием похищенных подлинников. Практикуются еще такие замечательные сделки, как продажа квартиры нескольким покупателям одновременно (продавец использует нотариально заверенные копии или имеет поддельные документы в нескольких экземплярах) или продажа незаконно присвоенной квартиры. Случается, что продается квартира, принадлежащая на праве собственности нескольким лицам. Один из них может присвоить всю сумму стоимости квартиры и скрыться.

Иногда покупателю показывают не ту квартиру, которую продают. Бывает, что фигурирует одна квартира, а документы оформляют на другую. При этом мошенникам ничего не стоит перевесить номера квартир, часто на целом этаже или во всем доме. Бывали случаи, что меняли даже таблички с номерами домов и названиями улиц.

И самое распространенное мошенничество — продавец, получив деньги от покупателя, отказывается выписаться из квартиры.

Весьма распространены и случаи реализации квартир не собственниками, а их арендаторами. Пользуясь поддельными документами, они получают аванс и скрываются.

Нередко квартиру продают по доверенности уже после того, как сам владелец жилья умер. Сделка после этого, естественно, является недействительной.

Бывали случаи, когда клиента обманывали представители организованного преступниками бюро, которое после заключения серии нечестных сделок прекращало свою деятельность

либо перебазировалось в другой район под новым названием. Создаются фирмы и для оформления одной-единственной сделки, после чего они исчезают.

Как правило, ни один подобный вариант вам не грозит, если вы решаете вопрос о покупке или продаже квартиры с фирмами-членами профессиональных риэлтерских организаций и объединений и компаниями, работающими на рынке недвижимости более пяти лет.

Следует помнить, что при покупке или продаже квартиры ничего нельзя подписывать, не проверив все документы другой стороны, причем не просто их наличие, а полное соответствие юридическим нормам, даже если текст документа кажется безобидным.

Ни в коем случае не оставляйте свой паспорт и свидетельство о приватизации квартиры у посредников и иных лиц (арендаторов и т. п.).

Одновременно с вручением денег следует сразу переехать в купленную квартиру и сменить замок. Необходимо также добиться выписки всех квартиросъемщиков с приобретаемой жилплощади (естественно, до передачи денег). Недобросовестный продавец в этом случае не сможет ее вероломно занять.

Понятно, что и продавец, и покупатель (в зависимости от степени честности партнера) могут остаться без денег. Партнеры как бы заранее вынуждены относиться друг к другу с подозрением. Возможный выход: деньги заранее передаются (на хранение) в надежную риэлтерскую фирму, которая обязуется контролировать исполнение сделки и ее регистрацию (за посредничество со сторон взыскивается 5 % от суммы сделки). Функции такой фирмы может выполнить также банк, куда передаются подписанные сторонами условия передачи денег.

При расчетах целесообразнее пользоваться не наличными деньгами, а расчетным счетом. Оригиналы приватизационных документов должны находиться у собственников до момента завершения сделки.

При покупке квартиры в кредит с правом ее аренды тщательно рассчитайте свои возможности. В противном случае есть риск стать плательщиком пени: 1 % от задолженности за каждый день просрочки. Неуплата может привести к расторжению договора аренды и «конфискации» первоначального взноса.

Стоит опасаться людей, стремящихся сделать все срочно, минуя установленный законом порядок, берущихся за самостоятельное оформление необходимых документов.

15. «КОТ» В КВАРТИРЕ

О чем идет речь? Например, о том, что купленную вами квартиру продать вам мог человек, который состоит на учете в психоневрологическом диспансере. Или пациент наркодиспансера — алкоголик, наркоман и пр. Вы, не зная об этом, покупаете квартиру, а через некоторое время родственники этого человека отправляются в суд со справкой о его невменяемости и расторгают сделку. При этом суд, конечно, принимает решение о том, что покупателю квартиры должны вернуть уплаченные за нее деньги. Фокус, однако, в том, что сумма, указанная в договоре купли-продажи квартир, как правило, намного меньше той, которая реально была уплачена за квартиру. Это во-первых. А во-вторых, нет никакой уверенности в том, что даже эта сумма будет вам возвращена. По закону, сделки, совершенные с «психами», алкоголиками, наркоманами, могут опротестовываться в течение десяти лет. За это время уплаченные вами деньги будут потрачены, и вы их не вернете.

Не меньше хлопот может доставить и покупка квартиры, в которой проживал человек, отбывающий наказание в местах лишения свободы. Когда он «садится» в тюрьму, то выписывается из квартиры. Но при этом права на проживание в ней не теряет. Такую квартиру вполне могут продать вам. И только по прошествии нескольких лет спокойной жизни в новой квартире вы вдруг обнаружите, что купили «коммуналку». А теперь представьте, что сосед ваш только что вернулся из заключения, поселился в вашей квартире и никуда выезжать не собирается.

16. ПОДДЕЛКА ДОКУМЕНТОВ В МОМЕНТ КУПЛИ-ПРОДАЖИ ЖИЛЬЯ

В процессе заключения и оформления сделки купли-продажи квартиры вам приходится иметь дело с большим количеством

разных документов. Именно они служат основанием для совершения сделки, и именно с ними связаны разнообразные способы мошенничества.

К наиболее часто встречающимся способам подделки документов относятся:

- ➡ переклейка фотографии (подобную подделку внимательный гражданин может выявить сам, обратив внимание на несовпадение выдавленных букв на паспорте и на фотографии, написание реквизитов документа не специальными черными чернилами, а иными, нечеткость самой фотографии и пр.);
- ➡ использование листов различных паспортов в паспорте одного гражданина (в таких поддельных документах, как правило, не совпадают серии и номера паспорта на страницах, что внимательный гражданин также способен выявить самостоятельно);
- ➡ постановка поддельных штампов прописки (регистрации) в паспортах (характерными признаками данного способа подделки являются нечеткость самого штампа прописки, несовпадение адреса прописки и номера отделения милиции, отсутствие штампа выписки с другого адреса или несоответствие адреса выписки номеру отделения милиции, на территории которого находится квартира);
- ➡ использование смонтированных ксерокопий документов, удостоверяющих личность;
- ➡ использование заграничных паспортов, в которых не указан адрес прописки (регистрации);
- ➡ предъявление фальшивых платежных документов;
- ➡ предъявление фальсифицированных документов, подтверждающих владение квартирой.

Часто мошенники под предлогом оказания помощи при обмене или расселении получают от владельца квартиры генеральную доверенность на право совершать любые сделки с квартирой, затем оформляют договор купли-продажи квартиры без участия владельца и даже его выписывают из нее без ведома последнего. Иногда в целях незаконного завладения чужой жилой площадью обманщики используют фиктивные доверенности на право распоряжения недвижимостью.

«Обман по договору» обычно легко «проходит» с простыми бабушками и дедушками. Маклер заключает с ними договор для продажи или обмена квартиры. При этом — «чтобы процесс пошел быстрее» — оформляет недвижимость клиента на себя, после чего квартира тут же продается, и у пенсионеров начинаются проблемы.

Оказывается, что в «умном» договоре, составленном на русском языке, отсутствует пункт о материальной ответственности маклера. Поэтому мошенник без зазрения совести исчезает с деньгами. А когда к нему приходит милиция, честно во всем признается:

— Да, все деньги я потратил, но обязательно отдам, когда смогу.

Доказать вину такого маклера оперативникам нереально, потому что аферист покажет настоящий договор с доверенностью...

17. ПРОДАЖА КВАРТИРЫ «ПОД ПРИНУЖДЕНИЕМ»

Довольно часто подаются иски о признании договора купли-продажи квартиры недействительным как сделки, совершенной под влиянием насилия и угроз.

Что это означает на практике? Продавец квартиры заранее договаривается с родственниками или знакомыми об определенном поведении на суде, затем продает квартиру и спустя некоторое время подает иск в суд о признании договора купли-продажи недействительным на том основании, что он совершил сделку под влиянием угроз со стороны тех лиц, с которыми он заранее договорился. На суде, естественно, «жертва» и «принуждающий к совершению сделки» действуют сообща и разыгрывают «спектакль». Исход дела зависит от того, насколько правдоподобно это будет происходить и удастся ли убедить суд в том, что дело обстояло именно так.

При продаже квартиры, являющейся общей совместной собственностью супругов, необходимо согласие другого супруга. Однако вполне реальна ситуация, когда супруги решают «нажиться» на продаже квартиры и заранее договариваются о совместных действиях.

Допустим, квартира была куплена в период брака, но оформлена на одного из супругов, и второй в ней не прописан. Если в паспорте супруга-продавца стоит штамп о регистрации брака, то нотариус обязательно потребует согласие на сделку второго супруга. Однако паспорт можно «потерять» и взамен получить «чистый», без штампа о регистрации брака. В этом слу-

чае после совершения сделки второй супруг может подать иск в суд о признании сделки недействительной на том основании, что у него не спросили согласия, а он был против. В итоге суд все вернет на свои места, а покупателю будут возвращены (возможно) деньги в сумме, оговоренной в договоре купли-продажи.

Недействительным может быть признан договор купли-продажи квартиры при признании недействительным первоначального договора передачи квартиры в собственность. В этом случае также может иметь место злонамеренный сговор проживающих в квартире лиц.

Хотя и редко, но все же возможны ситуации неправомерного завладения квартирой без ее оплаты (полной, частичной или заранее оговоренной суммы). При покупке квартиры мошенник просто не выплачивает деньги, — всю сумму либо часть обещанной суммы за совершение сделки. При этом нередко потерпевшими становятся социально деградированные личности (пьяницы, наркоманы), слабоумные старики, душевнобольные.

Мошенники для получения согласия на приватизацию и оформление документов или доверенности на право заключения сделки используют весьма разнообразные способы воздействия на граждан — от «стимулирующего» подталкивания к добровольному согласию (клиента могут спаивать, незаметно применять психотропные средства) до прямой угрозы физической расправы, пыток.

18. АГЕНТЫ-МОШЕННИКИ

Вы, наверное, знаете, что сегодня число желающих сдать квартиру намного превышает спрос на аренду жилья. Однако «прозванивая» по объявлениям, вы обязательно натываетесь на посредников.

Количество фирм и фирмочек, занимающихся посредничеством при сдаче квартир в аренду, учету не поддается. Желаете снять квартиру? Пожалуйста, нет проблем. Агентство, к примеру, предложит вам купить распечатку с перечнем сдающихся внаем квартир всего за каких-то 50 долларов. Вам представят длинный список вариантов. Что, есть сомнения? Позвоните наугад по любому телефону и сами

убедитесь, что хозяин квартиры хоть сегодня готов заключить сделку.

Но, когда деньги посреднику уже уплачены, может начаться настоящее кино. Приехав по указанному адресу, вы вдруг узнаете, что квартира либо уже сдана, либо вы просто «не проходите по конкурсу». То ли лицо у вас не той национальности, то ли семейное положение неподходящее, то ли пол не тот. Словом, причина для отказа всегда найдется.

А секрет в том, что хозяева всех этих квартир давно в сговоре с агентством. Они вообще ничего и никому сдавать не собираются, получая небольшой процент от той суммы, которую вы оплатили за липовую распечатку.

Уличить агентство в обмане практически невозможно. Пойди, докажи, что все это подтасовка!

Но обычно на такие аферы идут фирмы-однодневки. Солидные агентства дорожат своей репутацией. Поэтому, вознамерившись снять квартиру, поинтересуйтесь, есть ли у фирмы лицензия на этот вид деятельности, узнайте, давно ли она получена. Доверять, как правило, можно только тем, кто работает на рынке не менее пяти-шести лет. В ином случае вы просто оплатите не информацию, а фиговый листочек.

ГЛАВА 4

ТУРИСТ — ИДИОТ ПО ОПРЕДЕЛЕНИЮ?

Отдых — индустрия доходная. Человек, который весь год пашет коню подобно, вдвойне мечтает о том, чтобы в отпуске «оттянуться по полной».

А знаете почему «кидалово» в туристической сфере бизнеса обычно проходит безнаказанным для мошенников? Потому, что занятой и состоятельный человек ругаться из-за некачественного сервиса не станет. Не до того ему, бедолаге, ведь надо возвращаться в свой офис и опять погружаться в работу, а не судиться с туроператорами.

Итак, учимся правильно отдыхать.

19. АГЕНТСТВО И «АГЕНТСТВОЧКО»

Туристические агентства есть в каждом городе, но это еще не значит, что путевки нужно покупать именно в родных местах. Туристический бизнес построен таким образом, что, чем дальше находится агентство от столицы и чем оно мельче, тем дороже в нем путевки.

Конечно, нет смысла пытаться сэкономить на автобусном туре в Чехию или Польшу. Билет до столицы обойдется почти в такую же сумму, но для покупки турпутевки в Лондон, Париж или тура по Италии лучше выбрать серьезную столичную фирму.

Почему? Потому, что каждый год проходит большая туристическая ярмарка, на которой крупные туристические фирмы (торгующие путевками только оптом), отели и пансионаты выставляют свои предложения, а туристические компании скупают пакеты путевок на год, а потом уже предлагают их нам. Естественно, что чем крупнее и известнее компания, чем больше путевок она продает, тем большие у нее скидки, тем дешевле у нее путевки и качественнее ее сервис. В любой области лучше иметь дело с компанией, которая зарабатывает на обороте, а не на максимальных накрутках.

В результате какая-нибудь провинциальная «турфирмочка», которая не в силах приобрести пакет хороших путевок в разные страны, скупает их уже мелким оптом через третьи руки или заключает договор со столичной фирмой, делает наценку на путевку в 200—300 долларов и продает их в родном городе. Таким образом, получается, что, доехав на поезде до столицы, вы сэкономите только на стоимости путевки от 100 до 200 долларов (при том же качестве сервиса), которые можно успешно потратить в стране назначения на подарки и сувениры домочадцам.

Провинциальные турагентства, по крайней мере, честно зарабатывают свой хлеб, но в любом городе вам могут попасться и совсем нечестные ребята, которые попросят аванс за турпутевку и растворятся, а в лучшем случае отправят вас совсем не в тот отель, в какой обещали, забудут об экскурсиях, которые привлекли вас в рекламном проспекте.

Запомните несколько правил приобретения туров:

- ➡ никогда не покупайте путевки у мелких и неизвестных турфирм;
- ➡ не верьте, если вам скажут, что только сегодня вы стали счастливым обладателем супердешевой путевки куда-либо. Скорее всего стоимость

- перелета туда и обратно, которую вам нужно будет оплатить, превысит стоимость путевки, а в отеле вам выделяют далеко не лучший номер — разумеется, без развлекательной программы и шведского стола;
- ➡ сразу отказывайтесь от предложений, которые нужно оплатить «только сегодня до пяти часов». Скорее всего, это лохотрон;
 - ➡ попросите у туроператора ксерокопию лицензии (туристическая деятельность лицензируется в обязательном порядке), а если вам ее не дают, уходите, не раздумывая. Лицензию можно проверить в лицензионной палате, которая, собственно, эти лицензии и выдает;
 - ➡ опросите знакомых, поищите информацию в Интернете о турфирмах, а также поинтересуйтесь отзывами тех, кто уже куда-то ездил. Так вам легче будет определиться не только с местом, куда ехать отдыхать, но и с набором сервисных услуг, которые сильно влияют на стоимость путевки. Не слишком доверяйте и «звездности» отелей. В той же Турции или Египте трехзвездный отель покажется вам пределом курортных благ, так стоит ли платить в полтора раза больше за дополнительные «звездочки», если вы будете в отеле только ночевать, весь день проводя на пляже, в магазинах или рассматривая местные достопримечательности? С таким же здоровым скептицизмом можно отнестись и к «кормежке»: по-настоящему удобен в отеле только завтрак, все остальные запланированные приемы пищи туристы, как правило, пропускают из-за тех же шопингов или экскурсий;
 - ➡ многие туроператоры работают не самостоятельно, а входят в свои «профессиональные» союзы и ассоциации (так им легче покупать крупные пакеты путевок и перебрасывать друг другу горящие предложения). Как правило, у каждой ассоциации есть свои системы скидок, сезонные предложения, и вам следует обязательно о них узнать. Если фирма входит в какую-то ассоциацию, то, скорее всего, она работает по соглашению между всеми фирмами об оказываемых услугах, скидках;
 - ➡ если у вас есть загранпаспорт, верные друзья и знание иностранного языка, а въезд в страну, выбранную вами, безвизовый, то смело решайтесь на поездку без турагентства. Посмотрите в Интернете, какие отели есть в том районе, куда вы собираетесь, купите билет в оба конца (это в два раза дешевле, чем покупать отдельно туда и обратно). Учтите, что во многих странах (например, в Турции или Египте) цену за оплату номера можно сбить в 2—3 раза, а в Германии или Франции — всего на 10—20 процентов. Чем дороже и престижнее гостиница, тем более «косым» будет взгляд ее представителя, если вы с ним начнете торговаться. Наиболее лояльны к постояльцам хозяева небольших и полупустых гостиниц, удаленных от мест скопления туристических масс. А экскурсии можно устроить себе самостоятельно. Русскоязычные буклеты с описанием достопримечательностей есть в продаже

практически в любой стране (как правило, они продаются около тех же достопримечательностей);

- ➡ у каждой туристической фирмы имеются приоритетные направления, по которым она работает. Остальные предложения вносятся в список для ассортимента. Лучше всего ехать в том направлении, на котором фирма специализируется;
- ➡ заключая договор, учтите, что в нем должны быть прописаны все нюансы. Выражение «это же и так понятно» или «у нас стандартный бланк договора» говорит о том, что, если вас не устроит качество сервиса, никакие ваши претензии не будут приняты, потому что по договору фирма ответственности за них не несет. В договоре обязательно должен быть пункт об ответственности агентства за некачественный сервис и размере компенсации, которую оно выплачивает клиенту, если его что-то не устроит во время отдыха (обычно сумма компенсации — это процент от стоимости путевки, вплоть до полного возмещения оплаченной клиентом суммы);
- ➡ если по прибытии в страну отдыха вы увидели совсем не то, что ожидали и что было прописано в договоре, «подбейте» товарищей по несчастью вступить с фирмой, которая вам продала путевки, в переговоры по поводу возмещения части суммы, оплаченной за тур. Не забудьте, что в случае судебного разбирательства вам понадобятся доказательства, например, свидетельства работников и администрации отеля.

И вот, наконец, вы в вожаделенной стране, но расслабляться не стоит. Шарлатанов и просто коммерческих людей, не желающих упускать лишнюю копейку, хватает везде. Во многих странах принято торговаться, и продавец сразу называют цену в два-три раза выше, чем хотят получить. Но стоит ли ехать за рубеж только за тряпками? При сегодняшнем ассортименте наших магазинов привычка покупать вещи за границей — всего лишь дань «дефицитному» советскому прошлому. Тем более что даже во Франции, Италии или Германии во всех магазинах «одежды на каждый день» продается турецкая или китайская продукция, а «фирма́» — только в фирменных и дорогих универмагах, цены в которых не очень отличаются от московских. Так стоит ли тратить время на то, что в изобилии есть на родине? Вы ведь не челночник, а турист, так наслаждайтесь видами удивительных стран и городов.

20. МОШЕННИЧЕСТВА В ХРАНИЛИЩАХ БАНКОВ

Некоторые банки принимают от своих клиентов, а это часто касается именно туристов, отбывающих в дальние страны,

на безопасное хранение ценные бумаги, важные документы и материальные ценности. Таким предметам обеспечивается та же безопасность и защита, что и собственности банка, однако при отсутствии необходимого контроля возможны мошенничества и в подобных надежных хранилищах.

Среди мошенничеств в банках наиболее распространено проникновение в камеры для хранения в отсутствие владельца. В большинстве случаев неправомочный доступ банковских работников к камерам хранилища осуществляется с помощью тайно изготовленных дубликатов ключей клиентов, ключа клиента, который оставляет (по лености или излишней доверчивости) служащему банка. Убытки от неправомочного доступа к камерам хранилища обычно обнаруживаются при проверке клиентами своих камер. Клиенту бывает очень трудно доказать факт хищения из его камеры. Если не найден похититель, возмещение ущерба клиенту весьма сомнительно. Поэтому свой ключ не стоит никому передавать даже внушающим очень большое доверие людям.

Практикуется и хищение комиссионного сбора за аренду камер. Такие убытки обычно возникают при отсутствии контроля за доходами хранилища, когда служащий может присвоить наличные деньги, уплачиваемые клиентами за пользование камерами.

При проверке легко обнаружить, что некоторые из «пустых» камер были сданы внаем, так сказать, конфиденциально, без надлежащего оформления и получения банком дохода. Проверка также может показать отсутствие наборов ключей для не зафиксированных как сданных клиентам камер.

Предупредить убытки от мошенничества в хранилищах для клиентов можно прежде всего за счет жесткого контроля за работниками хранилища.

21. БИЛЕТИК ВНЕ ОЧЕРЕДИ

Расхожая ситуация — вы в незнакомой стране, пусть даже в условно незнакомой, например, в Украине или в Беларуси. Все, что вокруг написано и говорится, — вроде понятно, однако деньги не свои, «иностраные». И вы не можете автоматически соотносить в уме, сколь разумны предлагаемые вам цены. Не зря ведь психологи говорят, что за границей даже

очень прижимистые люди становятся более щедрыми и впадают в шопинговую паранойю, потому что иностранную валюту тратить легче.

Особенно часто жертвами вокзальных мошенников становятся или командированные, или люди, которые приобретают обратный билет сами и сразу, а не в рамках туристической группы.

Ваша поездка подходит к концу. У вас еще осталось некоторое количество денег и все вроде рассчитано. Вот вы приходите на вокзал и первым делом видите очередь, такую длинную, что у вас от уныния голова начинает кружиться. Вы приближаетесь к очереди, и тут к вам подсакивает молодой человек с лицом, внушающим доверие, и говорит — с билетами, видите, какая напряженка, давайте я вам без очереди все сделаю, только с маленькой накруточкой — примерно, как разница между общим вагоном и плацкартным. Все это молодой человек говорит на едином дыхании. А вы хорошо знаете, что, если за услугу заплатить чуть больше, пусть и «неофициальному» лицу, качество ее будет более высоким. Вы соглашаетесь, не трудясь предварительно узнать, сколько стоит билет, например в «гривнах», и сколько нужно уплатить молодому человеку. И вот он уже с билетом, стоит рядом, улыбается. Билет действительно хороший, в середине вагона, самый удобный поезд...

Чуть позже вам придется задаться вопросом — зачем все-таки вы заплатили 40 долларов за билет, который стоит 12 долларов? И который, будь вы не столь торопливы, спокойно приобрели бы в кассе, постояв в очереди?

ГЛАВА 5

Выйти удачно замуж

Несть числа отечественным золушкам, которые искренне верят в то, что постсоветские, славянские невесты — самые желанные и вожделенные для иностранных женихов. Во-первых, потому, что Хемингуэй когда-то написал, что русские девушки — самые красивые, во-вторых, потому, что наши соотечественницы

хорошо знают, что, в отличие от западных «эмансипе», они хорошо готовят, не гонят мужей, питаются в фаст-фудах, следят за собой, кроме того, они милые, нежные, кроткие... Одним словом, незачем размениваться на местных пьяниц, искать мужа следует в брачном агентстве, специализирующемся на выдаче россиянок замуж за рубеж.

22. ЖЕНЩИНА ДЛЯ «ФРАНЦУЗСКОГО ЛЕЙТЕНАНТА»

Итак, с чего начинается любое обращение в брачное агентство? С покупки газеты, где есть перечень таких агентств. Самые дорогие из них предлагают вам профессиональную фотосессию, консультацию психолога и адвоката для наблюдения за развитием будущего романа мы, конечно же, отмечаем — дороговато. Сами устроим собственное счастье.

Мы несем в агентство фотографию, изъятую из семейного альбома, которую миловидная сотрудница «своднической» фирмы при нас вклеивает в свой каталог, платим 50 долларов и наспех заполняем договор, особенно в него не вчитываясь. Еще бы, не квартиру ведь продаем, зачем так дотошно изучать каждую закавыку.

И пропускаем, случается, такую фразу: если по факту знакомства вас с каким-либо мужчиной вы не обратились к агенту в течение трех суток или недели и не сказали, что «клиент» вам не подошел, следовательно, нужно порекомендовать другого, обязательства перед вами фирмы считаются выполненными.

Дальше начинается самое интересное. Уже на следующий день вам звонит сотрудница и доверительно мелодичным голосом говорит: «Вот знаете, Наталья, только что приходили три оч-чень интересных киприота, такие мужчины, знаете, высокие, подтянутые, один особенно... я сразу вам позвонила. Он так описывал, какую избранницу себе представляет, что я сразу о вас подумала. Я ему уже предварительно намекнула, что есть у меня на примете девушка (вы сразу забываете о том, что в свои 35 на «девушку» как-то не тянете). В общем, завтра в пять он придет (уже он, а не они), вы подойдите, пожалуйста, а там, если не захотите с ним встречаться, я как раз свободна буду, мы с вами еще альбомы полистаем...»

Вы как-то не очень задумываетесь о том, какой «сюрприз» предстанет перед вами завтра. Да и национальность «киприот» вам как-то мало о чем говорит. Но главное — завтра! Вы идете на свидание — конец бабьему одиночеству!

И вот вы приходите. И вот он перед вами. То ли один, то ли с друзьями... Нет, возможно, вы влюбитесь с первого взгляда. В любом случае он тут же предложит вам познакомиться поближе, вместе поужинать.

Дальше развитие ситуации может быть каким угодно. Рассмотрев вас поближе, он решит, что как-то вы не очень... и, накормив вас вкусным ужином, незаметно сбежит, оставив вас тет-а-тет с официантом и огромным счетом. Возможно, вы очень скоро станете близки и проведете вместе три незабываемые недели, пока длится его командировка. Возможно, вы друг другу не понравитесь, и он вскоре звонить вам перестанет. А вы, связавшись с агентством, услышите совсем не мелодичный голос вашей знакомой сотрудницы, которая скажет как отрежет — вас познакомили, все обязательства выполнили. Хотите еще — оформляйте новый договор и несите деньги.

Отсюда мораль: хотите замуж за иностранца — сделайте портфолио у профессионала и разместите свое резюме в Интернет на соответствующей странице. А приступая к неvirtуальному знакомству, проконсультируйтесь у адвоката.

ГЛАВА 6

АВТО-БЕНДЕРЫ И АВТОЛОХИ

Выдавая кредиты на покупку автомобилей, банки и страховые компании столкнулись с новыми видами мошенничества. Одним из самых распространенных вариантов обмана является получение кредита по чужим документам.

Однако если при покупке бытовой техники необходим только паспорт, то, чтобы приобрести машину, надо представить еще и водительское удостоверение. При этом служба безопасности банка проверит подлинность обоих документов по

милицейским базам данных. Так как в них поддельный документ не будет зафиксирован, в банке немедленно сделают соответствующий вывод и в выдаче кредита откажут. Мошенники, впрочем, могут обойти и это препятствие.

23. «МЕРТВЫЕ ДУШИ» И ЖИВЫЕ МАШИНЫ

Через служащих загса мошенники могут получить паспорт недавно умершего человека. Поскольку сведения о смерти человека в милицейские компьютеры попадают с опозданием, покойник еще долгое время числится среди живых. В документе переклеивается фотография. Далее аферисты через «своих» стражей порядка получают данные водительского удостоверения умершего и заказывают фальшивый дубликат.

Теперь такой соискатель кредита легко проходит через стандартную процедуру проверки. Ведь номер документа и паспортные данные являются подлинными и фигурируют во всех базах данных.

Чтобы машина не была продана еще не расплатившемуся с кредитом покупателю, банки, как правило, не выдают на руки паспорт технического средства. Но и это препятствие легко преодолевается злоумышленниками. Они получают в ГАИ его дубликат, мотивируя это тем, что техпаспорт якобы был утерян.

Дальше автомобиль снимается с учета и вполне легально продается ничего не подозревающему человеку. Проблемы с таким транспортным средством у него начнутся позже, когда в банке поймут, что их «банально кинули». Машина будет объявлена в розыск, и добросовестный покупатель рискует ее лишиться.

24. «СЕРЫЕ АВТОМОБИЛИ»

Есть и более интересная схема мошенничества, при которой жертвой аферы становится не банк, а страховая компания. Этим видом «предпринимательства» занимаются серьезные преступные синдикаты. При покупке автомобиля в кредит его обязательно страхуют, в том числе и от угона. Далее новый владелец отгоняет ее перекупщику, а в милицию подает заявление

об угоне. От посредника бывший владелец получает до 30 процентов от стоимости машины.

Важно при этом, чтобы у хозяина автомобиля были оба комплекта ключей, которые бы свидетельствовали о том, что машину именно угнали, а не отобрали злоумышленники. Тогда у страховой компании будет одним поводом меньше отказать в получении страховки.

Получив деньги от преступников, владелец получает еще, согласно договору с банком, и новую машину. Из милицеской статистики известно, что раскрываются такие преступления крайне редко. Подобные махинации заставляют банки предъявлять достаточно высокие требования и проценты по потребительским кредитам.

Что же касается афер, связанных с полисами обязательного страхования автогражданской ответственности (ОСАГО), то, кроме «классической» схемы (преступники, подставляя свой автомобиль, получают деньги не с якобы виновного, а с его страховой компании) существует еще ряд методов незаконного получения денег.

Схема этого мошенничества полностью скопирована с той, которую в свое время предложили бюргерам выходцы из России. В Германии содержать автомобиль старше пяти лет экономически невыгодно: слишком высокие налоги на подержанные машины, большие эксплуатационные расходы и т. д. Продать такую машину в стране тоже проблематично, поэтому остается одно — сдать ее в утиль, причем, делается это не бесплатно.

Предприимчивые россияне предложили немцам «покупать» у них автомобили за треть от их стоимости по следующей схеме. Получив деньги, хозяин передавал покупателю документы на машину и ключи. Иномарка спокойно пересекала границу, растаможивалась, обзаводилась новым хозяином в Москве. А спустя три месяца несчастный владелец прибегал в свою страховую компанию, хватался за сердце и писал заявление, что у него угнали его любимицу. Получив возмещение и добавив еще денег, он покупал новую машину.

Сейчас в российском Интернете словно грибы после дождя растут объявления о покупке дорогих престижных иномарок по «немецкой схеме». Правда, в Москве причины, толкающие владельцев на такой шаг, — не высокие налоги, а мечта о другом автомобиле. Застрахованная машина также покупается примерно за треть, затем перегоняется на Кавказ, в Ингушетию.

Особой популярностью пользуются джипы любых моделей и «Мерседесы». Получив возмещение, «жертва угона» покупает себе другой автомобиль. Литва известна на всю Европу тем, что это самый дешевый кузовной автосервис. Буквально за копейки здесь могут из пяти машин собрать одну, восстанавливают такие автомобили, за которые в Москве даже профессионалы за большие деньги не берутся. Естественно, что многое делается по обходным технологиями, а собранная кое-как машина представляет реальную угрозу не только для тех, кто в ней сидит.

Схема аферы такова. Злоумышленник покупает в Москве разбитый автомобиль (речь идет о «Фольксваген-Пассатах», «Ауди А6», «Мерседесах» и «БМВ»), отвозит его в Прибалтику на «лечение», после чего возвращает в Москву, где страхует его от ущерба по рыночной цене, а затем «попадает» в серьезное ДТП и обращается в страховую компанию. По словам сотрудников ГИБДД, организациями подобных аварий занимается не один человек, а целые преступные сообщества, в которых есть водители-профессионалы или даже каскадеры. В качестве второго автомобиля выступает либо взятый на прокат, либо грузовик, который после совершения ДТП с места происшествия исчезает.

Эксперту страховой компании остается признать гибель застрахованного автомобиля, а преступнику и его сообщникам получить на руки деньги, да еще остаться с разбитой машиной.

По нынешнему налоговому законодательству страховщикам невыгодно забирать пострадавший автомобиль себе: для этого потребуется поставить его на баланс.

ГЛАВА 7

ПИРАМИДЫ ЕГИПЕТСКИЕ И ФИНАНСОВЫЕ

Но сначала немного истории...

Впервые «пирамида» была создана в США в 1919 году неким Чарлзом Понти, незадолго до этого эмигрировавшим в Америку из Италии. После целого ряда неудачных попыток

создать свой собственный доходный бизнес Понти создал новую фирму The Securities Exchange Company и, как полагаются, зарегистрировал ее в местной коммерческой палате (Chamber of Commerce). Было объявлено, что SXC привлекает средства внешних инвесторов для их выгодного вложения под высокий процент. Вообще говоря, всякие акции, облигации, векселя и другие финансовые инструменты рыночной экономики уже имели широкое хождение, и новый эмитент векселей никого не удивил. Вот только проценты SXC предлагала поистине сумасшедшие — по 45 процентов каждые девяносто дней.

Понятно, что остальные американские акции к такой высоте доходности не могли приблизиться даже близко, что и решило исход дела. Американцы стали активно вкладывать деньги в Securities Exchange Company. Первое время они и проценты получали исправно, что значительно расширило популярность SXC, а также резко увеличило приток новых вкладчиков. Все шло хорошо до 1920 года, когда, по причине возникновения у кредиторов Понти претензий на долю в SXC, власти штата были вынуждены начать судебное разбирательство и ознакомились с внутренней бухгалтерией компании. Тут-то и вскрылся обман. SXC никаких денег никуда не инвестировала, а просто платила проценты за счет поступлений от продаж новых выпусков своих облигаций. К счастью, XX век еще только начинался, и не существовало электронных проводок и международных офшоров. Так что деньги удалось найти и вернуть. В среднем каждый вкладчик получил около 37 процентов от номинальной стоимости векселя.

Однако на этом история финансовых пирамид не закончилась. Спустя семьдесят лет и две революции, уже в России идея финансовой пирамиды нашла благодатную почву для возрождения.

В 90-е годы XX века «МММ», «Русский Дом Селенга», АО «Русская недвижимость», «Тутти», «Ива́спорт», «Властилина» и другие «компании», пользуясь абсолютно аналогичными приемами, сумели обмануть более миллиона доверчивых россиян и жителей других государств СНГ.

Правда, в новых условиях итог оказался куда более печальным для вкладчиков. В подавляющем большинстве они потеряли свои вклады полностью и навсегда.

Казалось бы, финансовые пирамиды типа «МММ» или «Чары» ушли в историю, оставив миллионы обманутых вкладчиков ни с чем. Но жизнь показывает, что горький опыт оказался не столь поучительным для многих наших граждан.

Финансовые пирамиды продолжают существовать. Мошенники ищут новые формы обмана, при этом не очень-то рекламируют свою деятельность. Не лезут на экраны телевизоров, на страницы газет. Они идут другим путем.

25. КАК ПОПАСТЬ В «ПИРАМИДУ»?

Вот один из вариантов сомнительной возможности разбогатеть сразу и быстро, то есть попасть в пирамиду. Где-нибудь в подземном переходе или у входа в метро милые девушки раздают листовки с приглашением на высокооплачиваемую работу. Предложение просто заманчивое. Человек звонит по указанному телефону, ему сообщают, что как раз сегодня или завтра проводится презентация, милости просим.

Иногда клиента заманивают на эти презентации иным способом. У того же метро столь же миловидные девушки проводят маркетинговые исследования и в ходе беседы узнают номера телефонов потенциальных клиентов. Через несколько дней у вас дома раздается звонок, вам сообщают, что вы выиграли крупный приз, который будет вручен на презентации фирмы.

Итак, в указанный день и час в большом зале какого-нибудь клуба или учреждения собираются сотни человек, желающих получить высокооплачиваемую работу или обещанные призы. Сотрудники фирмы сообщают, что их компания занимается сетевым маркетингом, что она одна из крупнейших в своей области.

Что такое сетевой маркетинг? Многие присутствующие не имеют об этом ни малейшего представления. Но на них обрушивается шквал информации: об огромных заработках или доходах клиентов, о коттеджах, построенных ими на эти доходы, о приобретенных яхтах, бороздящих тропические моря, и тому подобное.

Представление продолжается. Выступают клиенты, обогатившиеся с помощью фирмы и утверждающие, что получить большие деньги очень легко. Правда, умалчивают, как конкретно это сделать. Посетителей уверяют, что сетевой маркетинг — прогрессивный вид бизнеса, широко распространенный в мире, в том числе в Европе, Японии.

Презентация длится несколько часов. Потрясающие перспективы завораживают многих. «Так что же требуется от нас?» — вопрошают они. Оказывается, очень немного. Надо сдать фирме всего лишь тысячу долларов, привести с собой еще трех клиентов, которые тоже принесут искомую сумму. Вот тогда-то денежки и потекут в ваш карман.

Взамен тысячи баксов человеку вручают бумажку, которая, конечно же, не относится к разряду ценных. Она не ликвидна, то есть взамен ее нельзя получить обратно свои деньги. Вот и все. Обычная финансовая пирамида. Кому-то повезет, и он получит некий доход. Но большинство клиентов, как это случилось со всеми, кто имел дело с пирамидами, останутся ни с чем, даже без своей кровной тысячи баксов.

В настоящее время наблюдается четкая тенденция маскировки финансовых пирамид под три легальных направления работы.

26. ПЛАТА ЗА «ЭЛИТАРНОСТЬ»

Суть этого направления деятельности заключается в создании неких элитарных закрытых клубов, члены которых предполагают получать высокие доходы от определенной деятельности.

Наиболее наглядным примером такого «клуба» можно считать сеть, созданную швейцарской фирмой «Астран». Ее основой являлись элитарные закрытые клубы, члены которых обязательно должны были иметь чрезвычайно респектабельный вид, платить высокие взносы (не менее \$1200) за право вступления и посещения клуба. Клубы весьма придирчиво выбирали будущих членов, исходя из их финансового состояния, внушаемости, готовности верить бездоказательным заявлениям, и сразу предупреждали новичков о необходимости скорейшего нахождения новичков, желающих вступить в клубное сообщество, иначе дивиденды не выплачивались. При этом члены клуба официально не покупали никаких акций или облигаций, а оформляли взносы как дарение некоторой суммы одного частного лица другому.

Благодаря тому, что клубы не стремились к мгновенному расширению, а также тому, что их организаторами на собраниях

членов скорее всего использовались приемы технологий нейролингвистического программирования (НЛП), подобные сообщества сети «Астран» вскоре появились во многих городах не только России, но и СНГ. Так, несмотря на относительную малочисленность, по данным прессы, только из Брестской области Беларуси на счета «Астран» поступило около 2 миллионов долларов. Во время обыска в брестском клубе был найден документ, в котором детально анализируются «ошибки» организаторов «МММ» и других «пирамид», а также даются практические рекомендации по организации работы «в новых условиях».

Похожие принципы применяются компаниями «Амарис», «Реванш», «Международный инновационный центр», «Константа», «Атлантида», «Золотой Меркурий», дислоцирующимися в Москве, Санкт-Петербурге, Екатеринбурге.

Нынешние финансовые пирамиды, в отличие от своих предшественников, не прибегают к громкой рекламе и не помещают никакой информации в газетах или на телевидении. Строжайшая тайна — вот девиз таких организаций.

Они не называются АО, ООО или ЗАО, а чаще всего выступают как бизнес-клубы для деловых людей. И попасть туда можно только через знакомых.

Итак, вам обещают хорошие деньги, свободный график работы, не требуются прописка и стаж. И приглашают на собеседование. За вход надо заплатить 300 рублей. «Но разве это деньги по сравнению с теми, что вам предстоит заработать? — говорит будущая жертва. — Ведь мой друг так изменился: стал респектабельнее, обозначились какие-то перспективы».

И вот жертва едет на собеседование. Как правило, оно проходит в красивом отеле или зале для презентаций. Больше двух раз в одном месте фонд не собирается. Жертву представляют, знакомят с «видными членами клуба», угощают кофе с пирожными и фруктами. Затем члены клуба рассказывают о своей социальной успешности. Вот медсестра. У нее не было денег, чтобы заплатить за вход, а теперь она открывает свой медицинский центр. А вот эта молодая девчонка завтра покупает новенькую «иномарку».

А потом начинаются семинары. Один за другим, в течение семи часов. Система «зарабатывания» такая: вы приводите двух человек и получаете за это 600 долларов. За третьего —

1000. Затем каждый из приведенных вами приведет с собой еще по два человека, и вы уже получите 1600 и 2600 долларов и т. д. Сумма может дорасти до 37 тысяч долларов. И только к концу дня вы узнаете, что сами должны заплатить вступительный взнос в размере 3400 долларов.

Подумать вам, вероятнее всего, не дадут, иначе вы можете выйти из-под контроля. Потому все делается быстро и в этот же день. И подобные истории происходят с очень богатыми людьми, которых трудно обвести вокруг пальца!

27. «ИНВЕСТИЦИОННАЯ» ДЕЯТЕЛЬНОСТЬ

Не менее эффективным способом является разделение пирамиды на несколько специализированных подразделений, большинство из которых занимаются внешне законной деятельностью и являются официально признаваемым источником получения прибыли. Примером такой структуры может служить деятельность системы «Сэкай». Вместо одной компании, была создана целая система организаций («Сэкай-траст», «Сэкай-инвест», «Сэкай-финанс», «Скоро», «Корогуми»), которые занимались инвестициями, финансовыми операциями и даже чисто торговой деятельностью.

Важной отличительной чертой таких систем, как «Сэкай», является их сильный религиозный уклон в область восточной мистики. Руководители «филиалов» и наиболее ответственные должностные лица в них назначались только из ближайших учеников гуру — учредителя, официально занимавшегося лишь духовным просвещением.

Тем не менее финансовой основой системы «Сэкай» была обычная пирамида, основанная на выплате премий ранее вступившим членам за счет взносов вновь вступивших. Всего, по данным следствия, таким образом было привлечено более 1 миллиона 200 тысяч долларов. Следует обратить внимание на то, что юридически каждый вкладчик «Сэкай» не покупал и не получал никаких финансовых документов (акций, облигаций, векселей и т. д.). В каждом конкретном случае оформлялась индивидуальная долговая расписка на сумму в 15—20 долларов между каким-либо из подразделений «Сэкай» и частным лицом. В результате, когда в 1996 году было заведено уголовное дело и начался суд, организатор «Сэкай» лично имел 3750 «заимодателей», многие

из которых продолжали надеяться на возврат денег и исков не подавали.

28. ПРОДАЖА «УСЛУГ»

Третья форма маскировки финансовой пирамиды сегодня имеет наибольшее распространение и минимально уязвима в юридическом отношении. Она заключается в продаже неких услуг, которые никогда не будут оказаны.

Примером подобной схемы служит деятельность страховой компании Si Save Invest Finanzierungs-Consulting, сфера интересов которой распространяется на всю территорию бывшего СССР и некоторых восточноевропейских стран.

Официально Si Save страхованием не занимается, а только распространяет с определенными изменениями на своих клиентов страховые услуги таких совершенно реальных и нормально действующих страховых фирм, как Grazer, Medlife, Fortuna, CMI и др.

Суть аферы заключается в том, что клиенту предлагается застраховать свое здоровье или жизнь на определенный срок, по истечении которого страховая сумма подлежит выплате в полном объеме. Прибыль клиента формируется за счет весьма большой разницы между объемом страховых взносов за этот срок и объемом страховой премии плюс начисленные проценты, если в течение действия полиса по нему ничего не будет выплачено. Сеть Si Save строит свою деятельность на том, что клиент, купивший полис на сумму более 1000 долларов, автоматически получает право продажи полисов третьим лицам. За каждого привлеченного клиента причитается премия, которая идет в зачет собственной страховки. Когда агент окупает свою страховую премию, он начинает получать реальные деньги.

Система Si Save ежегодно вывозит за пределы бывшего СССР 500—800 миллионов долларов.

Отметим, что под определение «финансовая пирамида» попадает не любое предприятие, чья маркетинговая деятельность основывается на сетевом способе распространения товаров или услуг, а только то, условиями которого клиент не может воспользоваться в данных конкретных условиях. Деятельность,

абсолютно законная в одном государстве, может быть финансовой аферой в другом, о чем свидетельствует схема Si Save.

29. КЛУБ «ЕДИНОМЫШЛЕННИКОВ» В ИНТЕРНЕТЕ

Примером подобных вариаций конечного смысла одинаковой деятельности являются другие компании, которые сегодня спекулируют на развитии Интернета и телекоммуникационных технологий. О них необходимо сказать отдельно.

Предлагая «сетевую» схему построения клиентской сети, такие компании дают своим клиентам возможность сделать выбор: вступить в клуб «единомышленников» с последующим правом самостоятельного привлечения новых клиентов и предоставлением личных скидок или получить сверхбыстрый доступ в Интернет посредством неких высокотехнологичных «боксов» (web-приставок к телевизору).

На практике речь идет о создании обширной клиентской базы для активной Интернет-торговли чужими товарами и услугами с собственного сервера. В условиях экономики и внутреннего рынка западных государств подобная деятельность не носит характера «финансовой пирамиды», так как «боксом» является обычная интернет-приставка (относительно дешевый компьютер с сильно усеченными функциональными возможностями). Она действительно позволяет войти в Интернет, а практика покупок товаров и услуг в сети на Западе является довольно привычной. Таким образом, в западных условиях, клиентам действительно предлагается сэкономить на разнице стоимости приставки и полноценного фирменного персонального компьютера, а также, по принятой там клубной системе, воспользоваться определенными скидками при покупке в виртуальном магазине данной компании.

Однако то же, но перенесенное в отечественные условия приобретает смысл финансовой пирамиды, так как эти компании никаких собственных каналов доступа в Интернет не создают, а конечные потребители, как правило, не имеют реальной возможности приобрести товары на сервере компании. В результате все, кто вступил в «клуб», рассчитывают исключительно на некую отдаленную перспективу (когда «все это

непрерывно зарабатывает») и на привлечение новых клиентов, что позволит вернуть вложенные деньги. Но 95 % «партнеров» не только не получают прибыли, а, напротив, — теряют и вложенные средства.

30. КАК СТРАХУЮТСЯ «СФИНКСЫ», СТЕРЕГУЩИЕ ПИРАМИДЫ?

В любой финансовой пирамиде нарастание долгов вкладчикам идет в геометрической прогрессии, то есть по экспоненте. И однажды наступает момент, когда долги за один шаг увеличиваются на столько же, сколько было долгов всего, за весь предыдущий период. Именно поэтому рушатся все пирамиды. Одни — раньше, другие — позже. Срок жизни пирамиды зависит лишь от количества втянутых в нее вкладчиков, промежутка времени между двумя шагами и стартовой суммы долга (сколько денег у вкладчиков собрано на первых шагах).

Что происходит в обычной пирамиде, когда ее руководство понимает, что больше не может выполнять свои обязательства перед вкладчиками?

Руководство скрывается, а для успокоения вкладчиков назначается абсолютно новый, никому не известный и не имеющий к пирамиде никакого отношения новый управляющий.

Что нужно знать человеку, заглянувшему на «тренинг» из любопытства? Напомним:

- ➡ финансовые пирамиды поддерживаются юристами и психологами;
- ➡ при входе на семинары иногда используют металлоискатели для обнаружения звукозаписывающих устройств;
- ➡ продолжительность семинаров составляет четыре часа и более, в течение которых постоянно звучит музыка, в зале раздаются аплодисменты;
- ➡ используется «особая» музыка, которая влияет на человека;
- ➡ подается чай, содержащий специальные травы;
- ➡ иногда используются гипноз, транквилизаторы;
- ➡ демонстрируются фильмы и ролики с кадрами «хорошей жизни»;
- ➡ организаторы обещают удачный бизнес, хорошую жизнь, круизы;
- ➡ во время выступлений произносится около 130 слов в минуту, тогда как для человека норма восприятия — до 90 слов в минуту;

- ➡ перед семинарами детально планируются действия каждого члена пирамиды;
- ➡ в зале людей рассаживают по предварительному плану: рядом с новичком должен сидеть член пирамиды.

ГЛАВА 8

КРЕДИТНЫЕ КАРТОЧКИ, ЭЛЕКТРОННЫЕ ПЛАТЕЖИ И ИНТЕРНЕТ

Преступления, совершенные с использованием пластиковых платежных средств, можно отнести к одним из наиболее опасных в экономическом плане, так как их негативное влияние отражается не только на работе самого банка, но и других субъектов.

Появление пластиковых платежных средств в системе безналичных расчетов породило новый вид преступлений.

Полноценный рынок пластиковых карт в странах СНГ еще не сложился, но совершенно очевидно, что все идет к его развитию и стабилизации, и поэтому недооценивать опасность преступлений и злоупотреблений в системе безналичных расчетов, по крайней мере, легкомысленно.

31. КРАЖА ПЕРСОНАЛЬНЫХ ДАННЫХ ВЛАДЕЛЬЦЕВ ПЛАСТИКОВЫХ КАРТОЧЕК

В последнее время участились случаи попыток кражи персональных данных клиентов различных финансовых структур — банков, аукционов и пр. Приведем один из классических способов кражи персональных данных. Он сводится к следующему.

Жертва получает письмо якобы от имени какого-либо аукциона примерно следующего содержания: «Уважаемый клиент! Вам нужно срочно обновить свои данные и ввести номер кредитной карты!..» и так далее. Как определить что письмо мошенническое? В этом может помочь следующая информация:

- ➡ мошенники не знают вашего имени, они рассылают свои сообщения как спам. Соответственно они обращаются к вам не по имени, а примерно так: «Уважаемый клиент». Официальные структуры же, если и напишут вам, то всегда обратятся персонально по тому имени, которое зарегистрировано в вашем профайле, например: «Уважаемый Вася Васин»;
- ➡ следует внимательно проверить, что скрывается под линком, по которому вам предлагается пройти на самом деле. А еще лучше никогда не «кликайте» на линк, а войдите в свой аккаунт обычным способом — открыв новое окно браузера и введя в строку адреса браузера адрес сайта вручную (не копируя линк). Зайдите в свой аккаунт. Если у вас действительно какие-то проблемы с вашим счетом, это будет помечено прямо на вашем счете. Письмо только дублирует эту информацию.

Данное преступление состоит в незаконном присвоении личной информации без ведома ее владельца для совершения мошенничества или кражи. Оно может совершаться по следующим схемам:

- ➡ злоумышленники открывают счет и оформляют новую кредитную карту, используя ваши украденные личные данные: имя, дату рождения, номер социального страхования. В результате неоплаченные злоумышленниками счета отражаются в отчете по вашей кредитной карте;
- ➡ аферисты звонят эмитенту вашей кредитной карты и, прикрываясь вашим именем, меняют почтовый адрес по вашему счету. Затем самозванцы начинают активно тратить ваши деньги, но так как теперь счета отсылаются на новый адрес, вы не сразу обнаружите обман;
- ➡ преступники открывают на ваше имя банковский счет и начинают выписывать чеки по этому счету. Случается, что жулики указывают открытый на чужое имя банковский счет как счет плательщика за услуги мобильной связи.

Поэтому, при получении по электронной почте письма от некоего Интернет-провайдера или поставщика информации с просьбой обновить или вновь ввести данные о своей кредитной карте для дальнейшей оплаты услуг, необходимо все тщательно проверить, чтобы не стать жертвой обмана.

На некоторых инвестиционных сайтах личная финансовая информация потенциальной жертвы может запрашиваться мошенниками для определения соответствия ее, то есть жертвы, статуса «аккредитованного инвестора».

Кроме имени и адреса электронной почты, злоумышленники могут попросить сообщить уровень дохода, информацию о банковском счете, номер социального страхования и другую персональную информацию.

Иногда в качестве уловки используется объяснение, что требуемые сведения необходимы для составления приоритетного списка (lead list) потенциальных инвесторов. Нужно проявлять максимальную осторожность, прежде чем сообщать о себе личные сведения.

Итак, нередко многие пользователи получают электронные письма с просьбой подтвердить свои банковские данные на специальной веб-странице из-за якобы возникших проблем технического характера.

В качестве примера можно привести электронное письмо, адресованное клиентам Сити-банка (CITIBANK) с темой «Important Fraud Alert from Citibank» («Важное сообщение о случаях мошенничества в Сити-банке»). В самом сообщении говорится о том, что в целях проведения операции, направленной на обнаружение нелегальной банковской деятельности, пользователям необходимо проверить правильность своих реквизитов на специальном веб-сайте.

Компания Panda Software вскоре предупредила, что все эти сообщения — фальсификация, их главная цель — получение конфиденциальной информации о клиенте (номерах счетов, именах пользователей, паролях и других секретных данных).

Рассылаемые сообщения были тщательно проработаны на языке HTML, чтобы максимально походить на оригинальные сообщения онлайн-банковской службы.

Фальшивые письма используют еще не исправленную URLspooф уязвимость браузера Microsoft Internet Explorer. Благодаря этой дыре пользователь думает, что веб-страница, к которой он обращается по ссылке из электронного письма, является официальным банковским сайтом, тогда как на самом деле это всего лишь точная копия оригинала, находящаяся на другом сервере.

Если пользователь введет запрашиваемые данные, они попадут прямиком в руки мошенника, создавшего это письмо и веб-страницу. Поэтому перед тем, как раскрывать свою конфиденциальную информацию, следует удостовериться в подлинности полученного сообщения.

32. ОПЕРАЦИИ С ПОДДЕЛЬНЫМИ КАРТАМИ

На данный вид мошенничества приходится самая большая доля потерь платежной системы. Ввиду высокой технической и технологической защищенности реальных карт самодельные карты в последнее время почти вышли из употребления, и их можно определить с помощью простейшей диагностики. Как правило, для подделки используют похищенные заготовки карт, на которые наносятся реквизиты банка и клиента. Будучи технически весьма оснащенными, преступники могут даже наносить информацию на магнитную полосу карты или копировать ее, то есть выполнять подделки на высоком уровне.

Аферы с поддельными картами характеризуются частичной или полной подделкой платежной карточки. Под измененными подлинными карточками подразумеваются карточки, изготовленные на имеющих соответствующее разрешение фабриках, но содержащие информацию о держателе карточки, отличную от той, которая имелась в первоначально выпущенной карточке. Частичная подделка пластиковых карточек совершается на основе использования подлинной карточки.

Механизм мошенничества может быть различным: мошенник получает в банке обычную карточку в законном порядке, вносит на специальный карточный счет минимально необходимую сумму. После этого (или до этого) он добывает необходимую информацию о держателе пластиковой карточки.

При подделке подписи используется несколько вариантов, но при этом учитывается то, что стереть образец подписи нельзя, так как при попытке это сделать в поле подписи проступит слово «недействительна». Поэтому ее часто просто закрашивают белой краской. Бывает, что поле подписи вообще меняют на новое с использованием самоклеящейся полоски бумаги.

Нанести добытую извне информацию о владельце на магнитную полосу и раньше в техническом плане не являлось большой проблемой. Данные просто вводились по принципу магнитофонной записи в соответствующем формате. Когда же эмитенты стали защищаться с помощью кодирования записи, родился скимминг — тщательное и полное копирование всего содержимого магнитных треков (дорожек).

Голограммы и эмблемы, сделанные по технологии дифракционной решетки, — не слишком эффективная защита, так

как во время рутинной процедуры идентификации на них обычно обращают меньше внимания, чем на подпись и прочие персональные реквизиты. Изменение эмбоossed (выдавленной) на лицевой стороне информации осуществляется разными путями.

Буквы и цифры, эмбоossed в плоскости карточки, мошенники могут срезать и с помощью клея заменять на другие. Таким образом, на карточке появляются совершенно новые номер и фамилия.

Один из самых опасных приемов подделки пластиковых карточек — производство полностью фальшивых карточек. Наиболее распространено полное копирование в некоторых странах Юго-Восточной Азии. Такой способ чаще всего используется организованными преступными группами, в которые, как правило, входят работники ресторанов и иных сервисных заведений. Они собирают информацию о кредитных карточках, которые попадают им в руки при оплате ресторанных и иных услуг, когда карточка на некоторое время исчезает из поля зрения клиента (как уже говорилось). А когда возвращается, у преступников на руках остается ее «брат-близнец».

К таким приемам относится и метод «чистого пластика» (WPC). Подделка карточки — дорогостоящая технология, так как степеней внешней защиты у настоящих карточек с каждым годом становится все больше (рисунки тонкими линиями, гильошированный слой, голограммы, фотографии, ультрафиолетовые картинки). При WPC на кусок чистой пластмассы в форме обычной карточки наносятся действительные данные (номер реального счета, срок действия, фамилия и т. д.).

Далее карточка используется владельцем сервисной точки, действующим вместе с преступной группой. Владелец магазина совершает фиктивный оборот, отправляет эмитенту карточки счета для оплаты, а прибыль делит со своими соучастниками.

С помощью «белых» карточек, заполучив PIN-код, можно совершать хищения, снимая наличные деньги через банкоматы, которые подпись не сличают, фото и другие атрибуты карточки не проверяют.

Кредитная информация, используемая при изготовлении поддельных кредитных карточек, может собираться в различных странах мира. Наиболее часто — в Канаде, Соединенных

Штатах Америки, странах Европы, а также из азиатского региона. Преступные группы, работающие в разных регионах, обмениваются такой информацией между собой.

В Омске при помощи поддельной карты были ограблены банкоматы Омскпромстройбанка системы «Золотая корона». Однако разработчики платежной системы смогли тогда убедить общественность, что речь идет о случайном доступе, не связанном со взломом систем защиты. В Омске состоялся судебный процесс — над молодым человеком, который сумел подделать микропроцессорную карту ОАО «Омская электро-связь», что окончательно развеяло миф о неуязвимости смарт-технологий.

33. ОПЕРАЦИИ С УКРАДЕННЫМИ ИЛИ УТЕРЯННЫМИ КАРТОЧКАМИ

Кража и мошенническое использование украденных пластиковых кредитных карточек остается наиболее распространенным преступлением. Методы противодействия им постоянно совершенствуются, однако в настоящее время компании предпочитают выпускать недорогие карточки с целью уменьшения суммы возможных убытков от их незаконного применения. Когда суммы убытков резко возрастают, компании предпринимают срочные усилия по введению новых мер безопасности.

Нанести крупный ущерб по украденной карте можно лишь в том случае, если мошенник знает PIN-код клиента. Тогда становится возможным снятие крупной суммы со счета клиента через сеть электронных кассиров-банкоматов до того, как банк-эмитент украденной карты успеет поставить ее в электронный стоп-лист (список недействительных карт).

Для указанного способа характерно завладение пластиковым платежным средством в результате похищения их у держателей путем кражи из квартиры, в транспорте или в других местах, а также в результате потери владельцем карточки после ее приобретения в банке и подписания.

В случае похищения карточки при пересылке ее по почте особенность мошенничества заключается в том, что владелец не знает об утрате карточки, не догадывается, что карточка у него похищена. Предотвратить хищение при этом способе

мошенничества очень сложно. Такой способ у нас пока не имеет распространения.

Из-за существенных потерь от почтовых краж многие организации, выпускающие карточки, пользуются для доставки заказными письмами. В качестве дополнительной меры предосторожности иногда посылают предварительное уведомление о предстоящей доставке карточки. Нередко вместе с предварительным уведомлением используется система, получившая название «двойное датирование». В этом случае карточка начинает действовать через месяц или более после даты отправки. В случае неполучения карточки этого отрезка времени достаточно для сообщения о пропаже и внесения карточки в список предупреждений. Некоторые организации, выпускающие карточки, требуют от получателя обязательного подтверждения о том, что карточка ему доставлена.

Если член преступной группы имеет возможность внедриться в почтовую организацию, то он получает уникальные возможности для кражи пересылаемых карточек, которые потом передает сообщникам. Таким образом, совершенствование способов доставки корреспонденции в сочетании с повышенными мерами охраны почты способствуют уменьшению краж пластиковых карточек.

По оценкам международных экспертов, самая мощная мафия, специализирующаяся на «пластиковом бизнесе», состоит из выходцев из Нигерии. В этой стране, по данным Интерпола, существуют не менее пяти крупных центров по подготовке профессиональных мошенников. После обучения способам мошенничества «выпускников» этих школ отправляют в страны Европы.

Здесь их встречают, устраивают на работу, как правило, уборщиками в крупные фирмы. Задача вполне определенная — сбор информации о конкретном человеке, обладающем солидным состоянием.

В компаниях, выпускающих карточки, обычно имеется круглосуточно работающая служба для сообщений об утере карточек. При получении сообщения счет клиента блокируется, и при всяком дальнейшем использовании его карточки проводится расследование. Иногда необычное количество транзакций может вызвать срабатывание компьютерной системы сигнализации еще до того, как будет известно о краже карточки. Проведенные исследования показывают, что сообщения об

утере карточки могут поступать в компанию даже через 3—4 дня после ее исчезновения, а в случае использования поддельной карточки мошенничество может обнаружиться даже через 30—40 дней.

Западные компании регулярно издают бюллетени с перечнем номеров карточек, подлежащих изъятию, и рассылают продавцам так называемые списки предупреждений. В некоторых торговых заведениях стоит специальная аппаратура (point of sale) — компьютерные терминалы, которые позволяют проверить состояние счета клиента перед тем, как сделка будет совершена.

Однако данный способ мошенничества возможен и успешен и потому, что правоохранительные органы и торговые предприятия технически пока еще очень слабо оснащены, и нет единой картотеки похищенных кредитных карточек, а также не всегда своевременно поступают в торговые организации стоп-листы.

Наиболее трудный случай для расследования — наличие сговора продавцов между собой или между продавцом и покупателем. Например, два продавца могут сотрудничать, обмениваясь утерянными или украденными карточками для проведения фиктивных транзакций. Продавец может также оформить продажу вещи мошеннику, которая на самом деле остается у него, а сумма, оплаченная финансовым учреждением, делится между ними по договоренности. Кассиру обычно предлагают 10—20 процентов от каждой операции, причем наличными деньгами.

Иногда кассиры вступают в преступный сговор с мошенниками из-за кажущейся безнаказанности криминальной сделки. Ведь единственный финансовый документ, подтверждающий операцию с пластиковой кредитной карточкой — слип (оттиск), на котором после обычной прокатки и остаются реквизиты пластиковой карточки.

Однако определить на глаз, считаны они были с настоящей пластиковой карточки или же просто с куска пластика с набитыми данными, практически невозможно. Этим и пользуются злоумышленники.

Есть еще одна разновидность мошенничества, которая подразумевает наличие непорядочного продавца или другого лица, располагающего номером телефона для проведения проверки карточки. Звонок позволяет выяснить, числится ли

карточка в списке похищенных или нет. Если нет, недобросовестный продавец может провести фиктивную сделку на крупную сумму через свое заведение. Если карточка числится украденной, он может осуществить несколько транзакций, не выходящих за пределы установленного ему лимита.

Мошенники располагают многочисленными способами использования украденных карточек. Организованные преступные группы платят от 100 до 500 долларов за украденную карточку, в зависимости от того, подписана она или нет, как давно украдена, находится ли она в списках украденных, как долго она использовалась законным владельцем, вычерпан ли лимит, есть ли дополнительные документы, удостоверяющие личность.

В большинстве преступных организаций вор продает украденную карточку «поставщику», который обладает необходимым количеством соучастников для ее использования. Члены группировки делают покупки с помощью украденной карточки согласно списку, заготовленного «поставщиком», следя за тем, чтобы стоимость покупки не выходила за пределы лимита, установленного для данного продавца. Приобретенные товары затем пересылается торговцу краденным для реализации.

Лицо, непосредственно совершающее мошеннические действия с карточкой, обычно получает около 40 % дохода, или ему позволяется использовать карточку для собственных покупок, прежде чем он вернет карточку «поставщику».

Разновидностью данного способа совершения мошенничества с пластиковыми карточками может стать использование карточки в преступных целях самим держателем, который, проделав крупные операции по карточке (чаще всего с банкоматом), может заявить, что карточка была похищена. В таких случаях привлекаются и сообщники, чтобы избежать возможности опознания.

34. МОШЕННИЧЕСТВО С ПОЧТОВЫМИ И ТЕЛЕФОННЫМИ ЗАКАЗАМИ

Данный вид преступлений появился в связи с развитием сервиса доставки товаров и услуг по почтовому или телефонному заказу клиента. Зная номер кредитной карточки своей

жертвы, преступник указывает ее в бланке заказа и, получив заказ на адрес временного места проживания, скрывается.

Подобным способом обычно добываются дорогостоящие предметы, такие, например, как компьютерное оборудование. Номера карточек можно узнать у персонала магазинов и ресторанов, из компьютерных бюллетеней.

Мошенническое использование номеров кредитных карточек включает широкий набор способов; один из них — мошенничество при помощи системы телемаркетинга и телекоммуникации. Поскольку для того, чтобы сделать заказ по почте или по телефону, не требуется предъявлять карточку, а нужно лишь сообщить ее номер, число вариантов способов мошенничества бесконечно и день ото дня растет. Злоупотребления в области телемаркетинга относятся к неавторизованным сделкам, совершенным телемаркетерами — мошенниками, а также преступниками, имеющими дело с настоящими телемаркетерами и предприятиями, принимающими заказы по почте.

В совершении преступлений в этой области принимают участие мошенники-телемаркетеры. Они различными способами узнают подлинные номера карточек и используют их при выписке поддельных счетов за заказы, оплата по которым зачисляется на банковский счет телемаркетера ежедневно. Поскольку большинство банков установили для счетов за заказы такой же режим, как и для наличных денег, телемаркетер имеет возможность немедленно переводить эти средства на другой счет или просто ежедневно снимать деньги со счета. Когда преступление раскрыто, телемаркетер-мошенник обычно исчезает вместе с деньгами.

Новой разновидностью такого вида мошенничества является использование сети Интернет для электронной системы заказов на различные товары. Однако уже сегодня насчитывается около 30 видов незаконных операций с пластиковыми картами через Интернет. Вот некоторые из них:

- ➔ оплата несуществующими карточками;
- ➔ создание фальшивых виртуальных магазинов;
- ➔ «электронное» воровство;
- ➔ фальшивые оплаты в игорных заведениях;
- ➔ многократное снятие со счета.

Данные преступления, как правило, совершаются работниками торговых и сервисных точек, принимающих платежи от

клиентов за товары и услуги по кредитным карточкам; осуществляют их путем оформления нескольких платежных чеков по одному факту оплаты. На основании предъявленных чеков на счет предприятия поступает больше денег, нежели стоимость проданного товара или оказанной услуги. Однако после совершения ряда сделок преступник вынужден закрыть или покинуть предприятие.

Указанный способ характеризуется участием в аферах обслуживающего персонала таких сервисных точек, как рестораны, кафе, бары, мотели и т. п. Работники подобных предприятий, пользуясь невнимательностью клиента или умышленно отвлекая его, производят несколько дополнительных оттисков пластиковых карточек (слипов), которые затем используют для присвоения материальных ценностей и денег.

Ключевым моментом в этом способе является то, что в отличие от магазина, где при расчете действия с карточкой происходят на глазах владельца, в ресторане официанты уносят ее на некоторое время, а после возвращают вместе со счетом.

При этом держатель карточки не догадывается, что предъявленный ему в качестве счета или вместе с ним слип — только один из нескольких, сделанных ловким кассиром или официантом.

От других оттисков его отличает лишь присутствие даты. В течение следующих нескольких дней наличные деньги, полученные с других клиентов, кассир, поделившись с официантом, может присваивать, а счета с реквизитами держателя карточки благополучно приобщать к отчетности и направлять для оплаты фирме-эмитенту (банку или платежной системе). При этом руководство заведения вполне может оставаться в неведении. Для избежания подобных действий пользователям карты рекомендуется внимательнее относиться к документам, подписываемым при совершении сделок даже на незначительные суммы.

35. АФЕРЫ С ИСПОЛЬЗОВАНИЕМ ПОДЛОЖНЫХ СЛИПОВ

Данный способ афер получил значительное распространение, и неперенным его атрибутом является соучастие кассиров

магазинов. Суть способа сводится к использованию заведомо подложных слипов, изготовленных путем применения поддельных клише или на основе наборных печатных форм, причем сведения берутся с подлинных пластиковых карточек. В этом случае чаще всего карточка используется без ведома ее законного держателя, который после выявления указанного факта не признает зафиксированные расходы.

Кассир получает от соучастников преступления заранее изготовленный слип, прокатанный в одну сторону (имеющий сведения о номере карточки, имени ее держателя и сроке действия) и дооформляет этот слип, прокатывая его в другую сторону, то есть проставляются данные о сервисной точке, через которую слип оформляется. После того как в кассу поступила оплата за какой-либо товар наличными средствами, в подложном слипе указывается в качестве оплаты та сумма, которая была получена наличными. Слип приобщается к отчету, деньги изымаются и присваиваются мошенниками.

36. МАХИНАЦИИ С БАНКОМАТАМИ

Внедрение автоматических кассовых аппаратов — мера весьма выгодная, так как их большая надежность и производительность по сравнению с живым кассиром делает их удобными и безопасными для широкого оказания услуг населению. Несмотря на это, преступники успешно нападают и на автоматические кассовые машины, применяя как чисто силовые методы (кража со взломом, полное разрушение и т. д.), так и мошеннические действия. В большинстве случаев используется настоящая карточка и настоящий персональный код, полученные злоумышленниками в результате кражи у законного владельца или обманом путем от финансового учреждения.

Известны случаи, когда злоумышленники звонят лицу, потерявшему карточку, и представляются инспектором банка. Якобы с целью проверки регистрации карточки они просят сообщить им персональный идентификационный номер, после чего счет становится доступным для кражи через кассовые автоматы.

Довольно часто при этом способе преступники идут на установление контактов с банковскими служащими, располагающими

информацией о денежных вкладах, о держателях пластиковых карточек с крупными вкладами (естественно за взятку).

До недавнего времени получение денег через банкомат было одним из наиболее надежных и безопасных способов использования пластиковых карточек, поскольку наличие PIN-кода, известного только пользователю, гарантирует идентификацию владельца карточки и конфиденциальность доступа клиента к счету. Однако международная практика уже зафиксировала изъятия крупных сумм через банкоматы.

Подключение электронного записывающего устройства к POS-терминалу/банкомату — новый вид мошенничества, зафиксированный в Венгрии. Этот вид преступления характеризуется полным копированием всего содержимого магнитной полосы пластиковой карточки.

Видимо, основным фактором для уменьшения убытков остается ограничение на денежную сумму (несколько сотен долларов), которая может быть выдана из одного автомата в течение дня.

Другой мерой предотвращения кражи являются специальные компьютерные программы, управляющие автоматической кассой. Вся информация, которой автоматическая кассовая машина обменивается с центральным компьютером, шифруется, чтобы предотвратить возможность подключения и перехвата сведений. Подозрительно частая выдача денег в течение короткого периода времени или неправильно указанный персональный номер могут привести к «проглатыванию» карточки автоматом.

Отдельным примером может служить применение злоумышленниками пластикового или металлического «рукава», специально подогнанного по размерам и вставляемого в щель банкомата для пластиковой карты. Когда пользователь вставляет карту в щель, она попадает в «рукав».

После введения PIN-кода транзакция не осуществляется; мошенник подходит к клиенту и говорит, что с ним случилось то же самое, и предлагает ввести код еще раз, и тогда карточку можно будет изъять. Жертва повторяет попытку, транзакция не проходит, и карта не выходит из банкомата. При наборе преступник смотрит и запоминает PIN-код. В конце концов, расстроенный клиент бросает карту в банкомате. Злоумышленник же специальным инструментом достает ее из банкомата и «очищает» счет клиента.

Возможно и такое — пользователь снимает деньги, а они не выходят. Это может означать, что мошенники заклеили скотчем внешнюю часть банкомата, которая выдает деньги (часть кэш-диспенсера). Пользователь нервничает, он уже и PIN-код набрал... Нехорошие слова слышатся в адрес сломанного банкомата, такие же в адрес банковских работников, с которыми утром он планирует поругаться. В состоянии чрезвычайной раздраженности человек забирает карту и идет искать другой банкомат. Из-за угла выходит злоумышленник, внимательно наблюдавший за жертвой, отклеивает скотч и забирает деньги. Прием простенький и незамысловатый, но иногда срабатывает.

В такой ситуации следует внимательно осмотреть кэш-диспенсер, и если никаких препятствий на пути купюр из банкомата в ваш бумажник не обнаружено, можно смело идти ругаться с работниками банка.

Самое трудное для мошенников — узнать PIN-код, что совсем непросто. И узнают его современные жулики способами адекватно непростыми. Даже способами промышленного шпионажа.

На клавиатуру банкомата накладывается специальная тонкая «маска» с микропроцессором, запоминающим нажимаемые цифры. На устройство, считывающее информацию с карты, также надевается соответствующее приспособление. Когда «жучки» снимаются, в распоряжении преступников оказываются все необходимые данные.

Иногда мошенники изготавливали и устанавливали фальшивый банкомат, внешне оформленный как многие другие, но, естественно, не работающий. Вернее работающий, но так, как надо мошенникам. При пользовании им законные держатели карточек оставляли свои реквизиты, включая данные о счетах, с помощью которых затем злоумышленники изготавливали поддельные карточки и получали наличные деньги через действующие банкоматы.

Чтобы избежать подобных неприятных моментов держателям пластиковых карт можно порекомендовать следующее:

- ➔ когда вы расплачиваетесь в магазине или ресторане, не выпускайте карту из виду;
- ➔ попросите, чтобы слип прокатали в вашем присутствии. Пусть принесут импринтер или сами подойдите к кассе. Иначе с вашей карты могут снять копию, а подделать вашу подпись не составит труда;

- ➡ если в магазине вам прокатали слип, но ваш банк не дал авторизацию или вы передумали делать покупку, проследите, чтобы ваш слип был уничтожен при вас. Ведь это оттиск вашей карты! И ничего не стоит вписать в него необходимую сумму, симитировать вашу подпись, а расчеты за подобную операцию повесить на вас;
- ➡ если первый слип плохо пропечатался, обязательно заберите бракованную квитанцию;
- ➡ при покупке карточки поинтересуйтесь наличием страхового полиса. Страховку берите всегда. Два раза банк просить не будет, а деньги за эту услугу вами, скорее всего, уже заплачены;
- ➡ никогда не пишите PIN-код на карте;
- ➡ никогда не храните записанный PIN-код вместе с картой. Лучше выучите код наизусть и вообще не храните его в письменном виде;
- ➡ обязательно оставьте образец своей подписи на обратной стороне карты сразу же после ее получения;
- ➡ никогда не передавайте карту другому лицу. В случае необходимости можно сделать, например, семейную карту, предоставив своим родным пользоваться деньгами на счету в пределах установленного вами лимита;
- ➡ никогда и никому не сообщайте свой PIN-код. Его не вправе требовать ни работники банка, выдавшего карту, ни обслуживающий персонал банкомата, ни следователь;
- ➡ не оставляйте карту без присмотра, например в машине, на столике в ресторане и пр.;
- ➡ никогда не сообщайте никому номер своей карты по телефону. Незнакомые, сколько человек услышат ваш разговор, и нет ли среди них того, кто может использовать услышанный номер в корыстных целях;
- ➡ при утере карты немедленно сообщите об этом по телефону. Если вы потеряли дебетовую карту, звоните в банк, который ее выдал. При утере кредитной карты одной из крупных систем следует сообщить по специальному телефону представителей платежной системы и в банк, выпустивший карту;
- ➡ проверяйте движения денег на вашем карточном счету. Проверяйте выписку по карте не реже одного раза в месяц. В этом случае вы успеете выставить претензию своему банку, а он — платежной системе. Существуют строго оговоренные сроки, в течение которых вы можете что-то предпринять. Особое внимание следует обратить на операции по счету после поездок, в которых вы пользовались своей картой.

Техника безопасности поведения у банкомата:

- ➡ старайтесь не пользоваться банкоматом в безлюдных местах или, наоборот, в местах, где наблюдается большое скопление людей. В

пустынном месте при снятии денег вы становитесь слишком уязвимым объектом для ограбления, в толпе нельзя быть уверенным, что никто не увидит вводимый вами PIN-код:

- ➡ не допускайте, чтобы вводимый вами PIN-код увидели посторонние люди. Не стесняйтесь закрывать от посторонних клавиатуру банкомата, а особо любопытных попросите отойти. В противном случае вполне возможно, что после этого вы обнаружите пропажу карточки, а чуть позже и денег с вашего счета;
- ➡ не ошибайтесь при вводе PIN-кода. После трех ошибочных вводов кода банкомат задержит вашу карту;
- ➡ будьте оперативны при общении с банкоматом. На каждую операцию дается определенное время — около 30—45 секунд. Если в течение этого времени операция не будет завершена, то в лучшем случае банкомат вернет вам карту, в худшем — задержит ее. Проверьте, все ли вы забрали из банкомата. После завершения операции у вас должны остаться: карточка, деньги, выписка о произведенной операции. Если чего-то не хватает, и банкомат не сообщил вам никакой дополнительной информации, то здесь что-то не так. Возможно, вы рискуете стать жертвой мошенников. Не доверяйте никому у банкомата, даже если этот человек одет в форму сотрудника службы по обслуживанию банкомата;
- ➡ всегда сохраняйте выписки по итогам операции, которые выдает банкомат. Это позволит вести учет снятых денег и контролировать списание денег с вашего счета;
- ➡ старайтесь не держать на виду свой бумажник и деньги, которые вы получили из банкомата. Не нужно их пересчитывать перед банкоматом. Машина не ошибается, а если и ошибется, то не ответит вам ничего вразумительного. А вот на окружающих вас людей пачка денег в руках может произвести неизгладимое впечатление с далеко идущими последствиями.

Техника безопасности при оплате картой в сети Интернет:

- ➡ старайтесь не оставлять данные о себе и своей карте на тех сайтах, о которых вы ничего не знаете. Спросите о них у друзей, знакомых. Поинтересуйтесь в соответствующих конференциях. Посмотрите, где располагается сама организация, которой вы собираетесь платить. Если адреса нет или он не вызывает у вас доверия, то прежде чем платить, стоит подумать, надо ли это делать;
- ➡ не используйте для оплаты в Интернете карты, на которых у вас находятся крупные суммы денег. Лучше вообще завести для таких целей отдельную карту и переводить туда деньги по мере необходимости;
- ➡ обращайте внимание на различные сертификаты, подтверждающие безопасность расчетов через данный сайт;

- ➔ при появлении малейших подозрений о неправомерном списании денег со счета, обращайтесь в банк. У вас есть определенный срок для того, чтобы отказаться или оспорить неправомерное списание денег с вашего счета. Продолжительность этого срока следует уточнить в банке, выдавшем вам карту.

37. АФЕРЫ В СЕТИ С КАРТАМИ И БЕЗ ОНЫХ

Инвестиционные аферисты пользуются Интернетом для продвижения старых и отработанных вариантов изъятия чужих денег. Впереди всех, разумеется, Нигерия с ее «деловыми предложениями», потом пирамидостроители, предлагающие сделать из 5 долларов 60 тысяч, для которых сеть — просто благословение божье, потому что «кликнув» раз, можно послать свой спам сотням тысяч людей, кто-то из них наверняка «купится».

За ними идут продавцы эквадорской недвижимости, нефтяных скважин в Антарктиде и кокосовых плантаций в Коста-Рике. Тут же крутятся «качки-кидалы», качающие деньги в покупку акций фирм, которые якобы сейчас пойдут в гору. После того, как все набирают себе этих акций, они кидают свою часть на рынок и уходят с прибылью.

Сеть глобализует все — и прибыли, и убытки, и глупость тоже...

В сфере электронной коммерции главная проблема заключается в точной идентификации участников транзакции и в защите сведений, составляющих ее содержание.

Высокий уровень афер в Интернете является сдерживающим фактором развития электронной коммерции (ЭК), поскольку покупатели, торговля и банки боятся пользоваться этой технологией из-за опасности понести финансовые потери.

Возможный тип мошенничества через Интернет может осуществляться через транзакции, выполненные злоумышленниками с использованием правильных реквизитов карточки (номер карточки, срок ее действия и т. п.). Для совершения транзакции электронной карты мошеннику обычно достаточно знать только ее номер и срок действия. Такая информация попадает в руки мошенников различными путями.

Наиболее распространенный способ получения преступниками реквизитов карт — сговор с сотрудниками торговых предприятий. Торговые предприятия, через которые проходят сотни и тысячи транзакций по пластиковым картам, зачастую хранят информацию о реквизитах карт в своих бумажных документах или на слипах. Результатом сговора становится передача информации о реквизитах карт в руки криминальных структур.

Например, в одной известной и довольно сложной афере покупателям предлагались дорогие видеокамеры по очень привлекательной цене, то есть ниже их стоимости на легальных сайтах, специализирующихся на электронной коммерции. Когда потенциальный потребитель вступает в контакт с «продавцом», «продавец» обещает отправить потребителю товар до того, как покупатель произведет оплату. Если потребитель согласен, «продавец» (без ведома покупателя) использует подлинное имя данного покупателя, а также полученный незаконным образом номер кредитной карты, принадлежащий другому лицу, для покупки товара на законном веб-сайте.

После того как такой сайт доставит товар покупателю, последний, полагая, что сделка законна, разрешает снять деньги со своей кредитной карты в пользу «продавца» или производит платеж непосредственно «продавцу». В результате пострадавших двое: электронный торговец, отправивший товар на основании незаконного использования кредитной карты, и потребитель, выславший деньги после получения товара, мошенническим образом заказанного «продавцом» у электронного торговца. Тем временем «продавец» уже мог перевести свою незаконную прибыль на банковские счета вне досягаемости торговца или потребителя.

Достаточно распространенным является способ, когда криминальные структуры организуют свои магазины и торговые агентства с главной целью получить в свое распоряжение значительные наборы реквизитов карт.

Часто такие магазины представляют собой различного рода порносайты. Сегодня западными спецслужбами установлена тесная связь порнобизнеса в Интернете с преступными группировками, специализирующимися на аферах с пластиковыми картами.

Другая функция подобных магазинов состоит в их использовании для «отмывания» полученных реквизитов карт. Через

подобные сайты «прокачиваются» сотни тысяч и даже миллионы украденных реквизитов карт.

Иногда обе функции — кража и «отмывание» — совмещаются в одном магазине. Например, воспользовавшись однажды услугами порносайта, владелец карты с удивлением выясняет, что стал подписчиком такого сайта, и, таким образом, с него ежемесячно будет взиматься плата за подписку, отказаться от которой весьма проблематично.

После того как в руках криминальных структур появляются украденные реквизиты карт, возникает задача ими воспользоваться. Один из способов — организация виртуального торгового предприятия, «торгующего» программным обеспечением или другими информационными ресурсами (это могут быть программы телевизионных передач, подписка на новости). В действительности такое торговое предприятие, как правило, имеет свой сайт, но ничем реально не торгует.

При этом в обслуживающий банк регулярно направляются авторизационные запросы, использующие украденные номера карт, а, следовательно, магазин регулярно получает от обслуживающего банка возмещения за совершенные в нем «покупки». Так продолжается до тех пор, пока уровень отказов от платежей, от эмитентов украденных реквизитов карт не станет свидетельством того, что речь идет об афере. Обычно к этому моменту и сами магазины, почувствовав запах жареного, исчезают и становятся предметом поиска правоохранительных органов.

Основная идея такой стратегии заключается в том, что действительный владелец карты заметит небольшую потерю средств на своем счете далеко не сразу, и в результате за имеющееся в распоряжении злоумышленников время (как правило, 1—3 месяца) можно на подобных небольших транзакциях украсть сотни тысяч долларов.

Наоборот, когда в распоряжении мошенников несколько десятков карт, выбирается стратегия выполнения транзакций на крупные суммы (несколько тысяч долларов). В этом случае активная жизнь псевдомагазина составляет несколько недель, после чего магазин исчезает.

Чтобы не попасть впросак, решившись на какие-то «денежные» действия в сети Интернет, есть смысл ознакомиться с рекомендациями, выработанными специалистами Internet

Fraud Complaint Center. Эти общие положения имеют универсальный характер, и, естественно, ими могут руководствоваться не только россияне.

Сводятся такие рекомендации к следующему:

- ➡ участвуя в Интернет-аукционах, помните, что об обязанностях покупателя (то есть вас) можно говорить только после того, как продавец выполнит свои обязательства;
- ➡ уточните, каким образом сайт-аукцион обеспечивает безопасность своих клиентов и гарантирует доставку им заказанных товаров. Спросите, есть ли страховка или иные гарантии того, что вы не понесете ущерба;
- ➡ узнайте как можно больше о продавце. Уточните, где находится его штаб-квартира. Изучите репутацию продавца. Известны ли случаи, когда он не выполнял своих обязательств? Для проверки репутации сайтов посетите Интернет-страницу авторитетной организации по защите прав потребителей Better Business Bureau: www.bbbonline.org/consumer;
- ➡ вас должна интересовать не только цена на необходимый товар. Обязательно внимательно ознакомьтесь со всеми примечаниями и сносками;
- ➡ узнайте, как вы будете рассчитываться за приобретенный товар. Если вам предлагают высылать чеки или денежные переводы на почтовый ящик (п/я), это ставит под сомнение надежность продавца;
- ➡ избегайте покупать товары на сайтах, базирующихся в других странах;
- ➡ поинтересуйтесь у продавца, как, когда и каким образом можно вернуть не понравившийся или бракованный товар, а также о стоимости и условиях доставки;
- ➡ уточните, кто будет доставлять товар. Это должна быть известная компания;
- ➡ всегда выясняйте, входит ли стоимость упаковки и пересылки товара в его окончательную цену;
- ➡ не предоставляйте продавцу свои паспортные данные — он абсолютно не нуждается в подобной информации;
- ➡ для пересылки лучше указывать свой домашний адрес, а не почтовый ящик или адрес офиса. Обязательно перезвоните продавцу и проверьте, точно ли он записал ваш адрес;
- ➡ если указан телефонный номер продавца, позвоните по нему в неуточное время. Если тот же человек снимет трубку — это хороший знак;
- ➡ лучше всего обмениваться информацией с помощью e-mail. Будьте осторожны, если продавец использует не персональный адрес электронной почты, а бесплатные почтовые ящики, которые предоставляют Hotmail, Yahoo и т. п.;

- ➡ не судите о репутации человека или компании по качеству сайта. Постарайтесь узнать о них что-либо еще;
- ➡ будьте особо осторожны, когда вам предлагают расплатиться с помощью кредитной карты. Используйте ее лишь в том случае, если проводите сделку через известный сайт с хорошей репутацией;
- ➡ иногда продавцы товаров на Интернет-аукционах предлагают договориться напрямую. Это может помочь сэкономить деньги, а может оказаться на руку мошеннику, поскольку такие аукционы часто обеспечивают страхование заключаемых на них сделок;
- ➡ никогда не доверяйте электронным «письмам из Нигерии» или любой другой страны, где предлагают за солидное вознаграждение помочь перевести деньги на зарубежный счет.

Кроме предложенных рекомендаций, стоит обратить внимание на следующие советы и деловые предложения:

- ➡ всегда проверяйте продавца прежде, чем предлагать свою ставку за лот. На некоторых сайтах аукционов есть специальные форумы, где можно прочесть отзывы и комментарии других посетителей относительно продавцов. Однако учтите, что положительные отзывы могли быть просто «сфабрикованы» продавцом, а отрицательные комментарии — всего лишь происки конкурентов. Негативные отзывы о продавце — это хороший предупредительный знак для вас, однако отсутствие жалоб не гарантирует, что ваша сделка на 100 % пройдет гладко;
- ➡ остерегайтесь «повышенной активности». Продавец может пробовать поднять цену искусственно, делая ставки под вымышленными именами или нанимая других людей для этой работы. Использование вымышленных покупателей незаконно и является нарушением правил аукциона;
- ➡ узнайте имя и контактную информацию продавца. Не вступайте в сделку с теми, кто отказывается предоставить эту информацию! Вы должны узнать имя, реальный адрес, e-mail и телефонный номер продавца, а также проверить эту информацию.

Есть очень много вариантов мошенничества на аукционах. Вот один из примеров.

Мошенник утверждает, что продает очень популярную вещь (на сегодняшний день это, например, ноутбуки, мотоциклы и автомобили) за подозрительно низкую цену. Злоумышленник получает достаточно информации о жертве, чтобы подать заказ на InExchange (обмен национальной валюты на e-gold) от имени жертвы, используя законный обменный пункт. Жертва производит оплату, думая, что обменный пункт

и есть то лицо, которое продает ноутбук, автомобиль, мотоцикл и т. д.

Обменный пункт, ничего не подозревая, принимает денежный перевод и выполняет обмен, не зная, что человек, который перевел оплату, — это не тот человек, который подал заказ на обмен.

Так как e-gold переводы являются безотзывными, то обмен не может быть совершен снова в обратную сторону. Это, в конечном счете, означает следующее:

- ➔ если денежный перевод был также безотзывным (например, банковский перевод), то жертва теряет свой денежный перевод полностью;
- ➔ если денежный перевод можно отозвать (кредитная карта, чеки и АСН платежи), то обычно жертва пытается уклониться от ответственности за свои действия, а это означает, что потери ложатся на обменный пункт.

38. МОШЕННИЧЕСКИЕ ESCROW-УСЛУГИ

Имейте в виду, что мошенники могут предлагать escrow-услуги, которыми якобы занимаются e-gold Ltd или G&SR. Однако, ни e-gold Ltd, ни G&SR не предоставляют escrow-услуги, а также не сотрудничают с escrow-службами. Поэтому стоит провести свое собственное расследование перед использованием любой службы escrow.

Схема escrow-мошенничества работает следующим образом:

- ➔ жертва находит на аукционе «сделку века». Ноутбуки и роскошные автомобили — самый типичный пример таких сделок;
- ➔ после того как жертва выиграла аукцион, продавец предлагает сервис escrow в качестве посредника. Продавец знает, что предложение использовать сервис escrow в большинстве случаев увеличит доверие покупателя к нему;
- ➔ продавец и владелец мошеннического сервиса escrow — одно и то же лицо;
- ➔ жертва заходит на мошеннический сайт escrow и подписывается на его услуги;
- ➔ злоумышленник высылает жертве письмо с фальшивой информацией относительно операции через escrow и дает жертве детальные инструкции о том, как открыть и пополнить счет e-gold;
- ➔ мошенник сообщает жертве о том, что надо уведомить его, как только счет будет пополнен. Жертва сообщает преступнику об этом. Тогда

мошенник создает новый счет в системе e-gold и отправляет свой номер счета назад жертве с инструкциями о том, как сделать перевод. Жертва делает перевод на этот e-gold счет и больше не получает никаких известий от службы escrow.

ГЛАВА 9

ИНВЕСТИЦИОННЫЕ АВАНТЮРЫ В СЕТИ ИНТЕРНЕТ

Каждый год в сети появляются миллионы новых инвесторов, оценивших простоту и доступность инвестирования с помощью Интернета. Однако их знаний и опыта часто бывает недостаточно для того, чтобы обезопасить себя и свои деньги.

Анонимность, которую предоставляет своим пользователям Интернет, возможность охвата большой аудитории, высокая скорость и гораздо более низкая стоимость распространения информации по сравнению с традиционными средствами ее передачи делают Интернет очень удобным инструментом различных авантур.

Онлайновое инвестирование как способ вложения денег получило самое широкое распространение за рубежом, особенно в США. Инвестиционная привлекательность и открытость фондового рынка США привели к значительному росту интереса к нему со стороны иностранных, в том числе и российских, инвесторов. Данная информация может быть полезна как для инвесторов, уже работающих или только рассматривающих возможность работы на американском рынке, так и для участников российского фондового рынка. Ведь наряду с положительными заимствованиями из практики развитых стран российский рынок неизбежно столкнется и с приобретением отрицательного опыта.

39. «ПИСЬМА ИЗ НИГЕРИИ»

Так условно окрестили сотрудники Интерпола весьма небезынтересный способ «глобального» вымогательства. Представьте,

что руководители средних и крупных компаний по всему миру получают письмо (факс, e-mail) от нигерийского бизнесмена, который выступает в роли посредника, представляя правительство своей страны. Подписываться же он старается впечатляюще: «принц», «директор» и т. д. В письме только в общих чертах говорилось, что бизнесмену необходимо перевести крупную сумму денег (от 10 до 30 миллионов американских долларов) в США, но счет открыть сам он по каким-то причинам не может. Все что требуется от вас — предоставить все необходимые сведения о своем банковском счете (счете фирмы), чтобы «принц» мог перевести туда свои деньги. За это вы получите «скромный» процент в размере 20—30 % от суммы (т. е. до 1 миллиона долларов).

Многие, наверное, догадались, что деньги, скорее всего, не чистые, однако желание быстро разбогатеть сделало свое дело. Представителей согласившихся сторон приглашали для закрепления договора в Нигерию, где их представляли «правительственным чиновникам», которые якобы должны были подтвердить перевод денег.

В процессе визита им говорили о необходимости — в качестве «жеста доброй воли», а также для взяток — внести небольшой вклад.

Иногда просьба превращалась в обычное вымогательство. Одного из бизнесменов заставили отдать 4 тысячи долларов в дорожных чеках, прежде чем он смог выехать из страны.

Суть же аферы заключалась в том, что перед решающим переводом миллионной суммы надо было заплатить в качестве гарантии «страховку» в несколько сотен тысяч долларов. Несколько человек даже успело перевести по 400 тысяч долларов «нигерийскому принцу», прежде чем стало известно об обмане. Естественно, что никаких 30 миллионов долларов никто не получил.

Несмотря на многочисленные публикации о подобных мошенничествах в прессе, предприниматели попадают таким образом по-прежнему.

К примеру, в фирму приходит письмо якобы от одного из высокопоставленных чиновников, отвечающего за распределение бюджетных средств в той или иной стране. Он предлагает — небезвозмездно — направить эти средства на закупку

товара именно этой фирмы, но просит предварительно перечислить относительно небольшую сумму для взятки некоему ответственному лицу. После такого перечисления контакты с чиновником прекращаются.

Некий «спецназовец» просил солидных получателей пссла-ния помочь ему вывезти найденные наличные с территории Афганистана, обещая за это приличный процент от общей суммы. Дождавшись, когда жертва клюнет на приманку, жулики через какое-то время сообщают, что для перевода или перевозки денег потребуются дополнительные расходы на адвокатов, налоги, разрешения и предлагают новым «партнерам» взять на себя эти «непредвиденные» суммы. Получив деньги, они бесследно исчезают.

Эта схема — разновидность хорошо известного приема злоумышленников, который в международных правоохранительных органах получил название «Нигерийская электронная почта» или «липа 419» — по номеру статьи Уголовного кодекса Нигерии, предусматривающей наказание за аферы. Официальное название этого преступления — «мошенничество с авансовыми выплатами».

40. «НАДУВАНИЕ ПУЗЫРЯ»

Это наиболее популярный и организационно очень простой в организации вид рыночной манипуляции. Аферист, выдавая себя за инсайдера, независимого аналитика или просто осведомленное лицо, распространяет заведомо ложную информацию о компании для формирования агрессивного спроса на ее акции. В результате искусственно созданного вокруг акций ажиотажа цена на них растет. Преступник получает возможность «снять сливки», продав свои акции по завышенной цене. После того как манипуляция произведена, цена акций возвращается на свой исходный уровень. Рядовые инвесторы терпят убытки.

Очень часто на онлайн-досках объявлений в дискуссиях и форумах для инвесторов можно увидеть сообщения, призывающие незамедлительно покупать или продавать акции той или иной компании до того, как их цена резко изменится. Обычно авторы подобных заявлений ссылаются на то, что они обладают «закрытой» информацией о важном корпоративном событии или используют «надежную» систему отбора «правильных» акций, основывающуюся на фундаментальном и техническом анализе. Единственное, что не сообщают авторы, так

это то, что они заранее купили эти акции по бросовой цене, чтобы затем продать их с хорошей прибылью на волне искусственно подогретого интереса.

Классическая реализация данной схемы на практике — «плетение паутины» ложной информации. На профессионально сделанном сайте некоей компании появляется «торжественный» пресс-релиз, сообщающий о финансовой устойчивости фирмы, о разработке нового товара или о внедрении инновационной технологии.

Тотчас же по электронной почте организуется рассылка «беспристрастных» рекомендаций, в которых акции компании фигурируют как самый привлекательный объект для инвестиций. Многочисленные сообщения в форумах и чатах призывают инвесторов поспешить с покупкой акций. Иногда благоприятные комментарии о перспективах компании можно услышать из уст «независимого» аналитика по радио или телевидению.

Чаще всего подобные аферы проворачиваются с акциями малых компаний, редко выставляемых на продажу. Ведь кроме низкой ликвидности и низкой цены манипуляцию с ними облегчает недостаток или отсутствие доступной достоверной информации о компании-эмитенте.

Популярны и так называемые горячие американские акции. Подобные аферы ориентированы на неопытных иностранных инвесторов. Их предметом становятся акции совсем мелких американских компаний (micro-cap stocks), отличающиеся низкой ценой и очень низкой ликвидностью, что делает их очень удобным инструментом рыночных манипуляций.

Нечестный брокер покупает у американского эмитента крупный пакет акций со значительной скидкой, а затем, используя тактику «навязывания» и давления, убеждает инвесторов покупать эти бумаги по весьма завышенной цене. После того как брокер получил прибыль, продав свой пакет акций по высокой цене, она резко падает, оставляя инвесторов, «обжегшихся на горячих акциях», в убытке.

Многие инвесторы осознают, что они стали жертвой обмана тогда, когда сталкиваются с невозможностью дозвониться или иным образом связаться с брокером, продавшим им злополучные акции. Он просто исчезает. Иногда мошенничество на этом не заканчивается и принимает новый оборот.

Преступники, выдавая себя за законопослушных американских брокеров, предлагают «обжегшимся» инвесторам помощь в компенсации их потерь через обмен их ничего не стоящих «бумажек» на акции крупных уважаемых компаний. Но сначала инвесторы должны внести авансовый «гарантийный депозит» или иным образом обеспечить выполнение своих обязательств. И до тех пор, пока инвесторы будут надеяться на возврат потерянных денег и платить за эту надежду, мошенники будут вымогать из них все новые и новые суммы, объясняя, что эти платежи пойдут на покрытие дополнительных сборов, налогов и прочих расходов.

Схема «безрискового вложения капитала», предлагаемая пользователю через сеть, состоит в распространении через Интернет заманчивых инвестиционных предложений, сочетающих обещание высокой прибыли с низким уровнем риска. Часто речь в них идет об участии в высокодоходных, но на самом деле несуществующих проектах, причем в случае неудачи предусматриваются якобы безусловные гарантии возврата вложенных средств.

Особенно популярны в таком виде мошенничества «экзотические предложения». Таковыми можно считать покупку акций кокосовой плантации или фермы по разведению морских угрей. Видимо, здесь преступники делают ставку на то, что инвесторов удастся ввести в заблуждение редкостью и необычностью подобных инвестиционных предложений. К данной категории можно отнести и сомнительные предложения по инвестированию в офшорных зонах. В безналоговых «гаванях» очень трудно проследить путь денежного перевода и найти счет, на котором в конце концов «осели» деньги.

41. НАВЯЗЫВАНИЕ ИНФОРМАЦИИ

Недостоверная информация может распространяться среди широкого круга пользователей сети самыми разнообразными способами.

Инвестиционные новостные рассылки. В настоящее время сетевым инвесторам предлагают сотни новостных рассылок (online newsletters) с бесплатной и на первый взгляд беспристрастной информацией о тех или иных компаниях, а также акциях, рекомендуемых в качестве наиболее удачных объектов для вложения средств.

Конечно, большинство онлайн-информационных бюллетеней действительно помогают инвесторам собрать ценную и достоверную информацию, но новостные рассылки могут служить и инструментом жульничества.

Некоторые компании платят составителям или авторам новостных рассылок вознаграждение в виде денежных сумм или собственных акций за то, чтобы они в благоприятном тоне упомянули и рекомендовали к покупке их акции. Хотя эта практика не является противозаконной, федеральное законодательство по ценным бумагам требует, чтобы в рассылках указывалось, кто выступает их «спонсором» и какое вознаграждение получают их авторы. Естественно, аферисты эту информацию не раскрывают, но высокопарно заявляют о своей независимости и неподкупности, говорят о выборе акций, который стал результатом долгих рыночных исследований, приводят свой длинный послужной список. На самом деле очевидно, что «независимые» консультанты получают хорошие деньги, если убедят инвесторов покупать или продавать указанные заказчиком ценные бумаги.

Доски объявлений. Онлайн-доски объявлений (bulletin boards) — будь то сетевые конференции или пользовательские сети (системы электронных досок объявлений, упорядоченные по группам новостей) — стали для инвесторов очень популярным способом обмена информацией. Но среди достоверных сообщений встречаются и такие, авторы которых преследуют цель несправедливого обогащения за счет обмана или введения в заблуждение других инвесторов. Мошенники часто используют этот механизм общения для манипулирования настроениями инвесторов. Ведь последним трудно проверить источник информации и его надежность, так как многие доски объявлений позволяют пользователям скрывать свое истинное имя под различными псевдонимами (никами). Поэтому в роли «беспристрастного» рыночного обозревателя может выступать заинтересованное лицо, будь то крупный акционер, руководитель компании или оплаченный «промоутер».

Всего один человек может легко создать иллюзию всеобщего интереса к малоликвидным акциям какой-нибудь неизвестной компании, разместив серию сообщений под различными именами.

Рассылка мусорных сообщений по электронной почте. Наладить рассылку мусорных сообщений (e-mail spam) достаточно легко и дешево. Поэтому мошенники широко используют этот прием для распространения ложной информации и в поиске жертв своих инвестиционных махинаций. Рассылка спама позволяет злоумышленникам охватить существенно больший круг потенциальных инвесторов по сравнению с телефонным обзвоном или рассылкой традиционных почтовых сообщений. Используя программу массовой отправки электронной почты, спаммеры могут направлять персональные сообщения одновременно тысячам и даже миллионам пользователей. В США был случай, когда аферист для манипулирования курсом акций перехватил посланное по электронной почте официальное сообщение должностного лица некоей корпорации, изменил его, добавив заведомо ложную информацию, а затем мгновенно разослал его миллионам людей.

Аналитические обзоры. Необходимо упомянуть и об осторожности в следовании рекомендациям рыночных аналитиков, обладающих известным влиянием на формирование умонастроений инвесторов. Аналитики — это чаще всего служащие инвестиционных и брокерских компаний, банков и прочих финансовых учреждений, занимающиеся рыночными исследованиями, оценивающие и отбирающие инструменты для инвестиционных операций. Большинство аналитиков специализируются на бумагах определенного сектора или отрасли экономики и выносят свои рекомендации в отношении целесообразности их покупки или продажи. Отчеты аналитиков, содержащие результаты их исследований, могут существенно повлиять на цену акций, особенно когда их рекомендации распространяются через электронные или традиционные средства массовой информации. И если известный аналитик даже вскользь упомянет о какой-либо компании, это может на какой-то период вызвать рост или падение ее акций, несмотря на то, что за последнее время не произошло никаких изменений ни в фундаментальных показателях компании, ни в прогнозах ее будущего развития. Основная роль аналитиков заключается в том, чтобы повышать эффективность работы рынка. Их задача — выявлять скрытые от глаз большинства инвесторов факты и закономерности, давать свою оценку развитию отраслей экономики и отдельных компаний. Аналитики предоставляют инвесторам важную и ценную информацию, снабжают их инвестиционными идеями.

Однако инвесторы всегда должны помнить о существовании потенциального конфликта интересов.

Некоторые аналитики работают на компании, выступающие андеррайтерами (подписчиками и распространителями новых выпусков акций) или акционерами корпораций, которые эти аналитики отслеживают.

Иногда сами аналитики напрямую или косвенно (например, через план покупки акций служащими, employee stock-purchase plan) являются акционерами изучаемых ими компаний. У работодателя могут возникнуть обстоятельства, оказывающие давление на объективность и независимость аналитика. И хотя существование подобных обстоятельств необязательно означает, что аналитик ангажирован или подкуплен, инвесторам при принятии решений следует иметь это в виду и не полагаться безоглядно на рекомендации рыночных «гуру».

42. ГЕНЕРАЦИЯ ТИТУЛЬНЫХ ЗНАКОВ WEBMONEY (WM)

Данные знаки в Интернете используют в качестве платежного средства, и их можно по желанию обменять на доллары или рубли, но тем не менее собственно деньгами WM не являются, на чем и основано самое масштабное в области WM мошенничество — прием WM под проценты.

Сначала фонды деньги возвращают, и действительно с процентами — за счет притока новых членов, а потом в один прекрасный момент просто перестают выполнять обязательства. Такие фонды объясняют свои высокие проценты игрой в торговле на рынке Forex.

Еще один тип афер связан с генерацией титульных знаков WebMoney. На сайтах пользователям кошельков (киперов) WM рассказываются научнообразные сказки, что в системе WebMoney обнаружена прореха, которая позволила создать программу, автоматически увеличивающую количество WM в кошельке пользователей. Эти программы предлагается купить за те же самые WM. В 100 % случаев это «троянский конь», который попросту вычищает подчистую кошелек пользователя.

Подобным образом действуют и липовые обменники WM. Для простого обмена WMZ на WMR и обратно предлагается

скачать и установить на свой компьютер специальную программу. Но и в этом случае вы можете остаться совсем без денег.

ГЛАВА 10

МАХИНАЦИИ С БАНКОВСКИМИ ОПЕРАЦИЯМИ

Привлеченные обещанием астрономических прибылей, возможностью поучаствовать в эксклюзивной международной инвестиционной программе или получить доступ к инвестиционным портфелям крупнейших банков мира, инвесторы часто становятся добычей «банковских» мошенников, прикрывающихся именами и гарантиями известных финансовых учреждений.

Организаторы данных схем используют слово prime (первоклассный) или синонимичные фразы, например top fifty world banks (50 лучших банков мира), «prime European bank» (первоклассный европейский банк), чтобы замаскировать аферы громкими заявлениями о том, что в этих высокодоходных инвестиционных программах («high yield investment program», HYIP) участвуют крупные и солидные финансовые институты. Иногда инвесторам обещается доступ к «секретным» инвестиционным инструментам, используемым Ротшильдами или членами Саудовской королевской семьи.

В банковской сфере злоупотребления со стороны персонала — достаточно распространенное явление. Мировая практика показывает, что в мелких банках аферы происходят гораздо чаще, чем в крупных. Это связано в первую очередь с совмещением в мелких банках одним человеком нескольких должностей, что позволяет совершить хищение в качестве кассира, а потом скрыть его в качестве бухгалтера.

Отечественные банки в большинстве своем по мировым стандартам являются мелкими. Кроме того, отечественный бизнес проходит сейчас этап высокой криминализации и мелкие банки легче подпадают под влияние криминальных структур или даже создаются ими.

Достаточно распространены клиенты, которые берут кредит заранее не намереваясь его возвращать («кидалы»). Работников

банков, имеющих небольшую по мировым стандартам оплату труда, часто можно легко подкупить.

Много и «карманных» банков, которые ориентированы на обслуживание своих учредителей. Таким учредителям часто даются фактически бесплатные кредиты, за возвратом которых не особенно тщательно следят.

В последнее время в России, Беларуси и Прибалтике учредители сами обанкротили значительное количество мелких банков. Схема была стандартна: после регистрации банка привлекались новые клиенты, переходившие на расчетно-кассовое обслуживание в учрежденный банк или клавшие в него деньги на депозит, активно привлекались ресурсы по межбанковскому кредитованию. После аккумуляции в банке достаточно солидной суммы учредителям банка выдавались особо крупные кредиты, которые в совокупности делали банк неплатежеспособным. Вскоре учредители выходили «из игры» (если успевали), а в убытках оказывались сторонние клиенты банка.

43. МАХИНАЦИИ С ПРОСТЫМИ ВЕКСЕЛЯМИ

Простой вексель — безусловное долговое обязательство — один из инструментов, с помощью которых компании заимствуют необходимые средства. Большинство афер с простыми векселями имеют следующую схему: злоумышленники, связанные или не связанные с компанией-заемщиком, убеждают независимых агентов по страхованию жизни, обещая им высокие (до 20 — 30 %) комиссионные, продавать своим клиентам простые векселя. Зачастую эти страховые агенты не имеют соответствующих лицензий на продажу ценных бумаг и, предлагая векселя потенциальным инвесторам, даже не подозревают о том, что выступают соучастниками мошенничества.

Инвесторам обещают высокий гарантированный доход с совершенно незначительным риском. Кроме того, привлекательность инвестиционного предложения может усиливаться ложными утверждениями, что векселя гарантирует или страхует некая иностранная страховая компания.

Иногда часть поступлений от продажи векселей идет на поддержание пирамидной схемы: деньги от продажи новых

партий векселей идут на оплату процентов более ранним кредиторам. Некоторые аферисты при наступлении даты платежа по векселям уклоняются от возвращения инвесторам основной суммы долга, убеждая их продлить кредит за счет покупки новых векселей. При такой схеме инвесторы в течение некоторого времени действительно могут получать обещанные процентные платежи, но вероятность того, что они когда-нибудь смогут вернуть себе основную сумму займа, практически равна нулю.

Часто аферы с простыми векселями ориентированы на пожилых людей, которые боятся потерять свои сбережения и поэтому с готовностью откликаются на инвестиционные предложения, сулящие получение гарантированного дохода при невысоком риске потерь.

Настоящие корпоративные векселя обычно не предлагают широкой публике, а распространяют частным порядком среди ограниченного круга опытных инвесторов, которые в состоянии проявить должную осмотрительность и самостоятельно изучить деятельность компании-заемщика. Поэтому совершенно не стоит доверять предложению по покупке корпоративных векселей, если вы прочитали о нем в Интернете.

Для проверки «вексельного предложения» на честность можно сравнить обещаемую по векселям доходность с текущими рыночными ставками для аналогичных инструментов с фиксированным доходом, с доходностью краткосрочных казначейских обязательств или депозитных сертификатов, застрахованных в Федеральной корпорации по страхованию депозитов (FDIC). Если доходность по предлагаемым векселям намного превышает доходность по упомянутым инструментам, велика вероятность, что вас хотят обмануть.

44. ОТЗЫВНЫЕ ДЕПОЗИТНЫЕ СЕРТИФИКАТЫ

Данные инструменты представляют собой обращающиеся ценные бумаги на предъявителя. Они свидетельствуют о наличии в банке срочного депозита на определенную сумму и обычно имеют сроки погашения от трех месяцев до пяти лет. Мошенники продают отзывные депозитные сертификаты, дата погашения по которым наступает через 10—20 лет. Кроме того, предусмотрено, что если инвестор желает досрочно погасить свой депозитный сертификат, он несет значительные потери, достигающие 25 % от суммы первоначального вложения.

При этом продавцы сертификатов не раскрывают всей информации о рисках, которые инвестор принимает на себя, и не предупреждают заранее о существовании ограничений в отношении досрочного погашения сертификатов.

45. РАСЧЕТНО-КАССОВОЕ ОБСЛУЖИВАНИЕ

При расчетно-кассовом обслуживании клиентов мошенничество совершается достаточно часто. Особенно широкие возможности для афер открываются при совмещении одним человеком функций бухгалтера и оператора.

Наиболее распространенным методом является фабрикация денежных документов, прикрывающих недостачу. После взятия денег из кассы «на время» и отсутствия возможности их вернуть вероятна фабрикация денежных документов на сумму недостачи (например, выписка расходного ордера).

Создается ситуация, что кассир якобы ошибся. Изымается небольшая сумма денег, докладывается о недостаче, которая будто бы возникла в силу ошибки в ранее сделанных расчетах, и предлагается переделать старые документы для достижения «полного ажюра». Таким образом похищаются небольшие суммы, но если умело «дурить голову» вышестоящему начальству, беспрекословно принимающему исправления, сумма может набежать довольно крупная.

Соккрытие привлеченного депозита — тоже вид мошенничества. Клиенту выдаются все необходимые документы о привлечении его денег на депозит, но эти деньги не оприходуются. По истечении срока депозита (а аферы обычно совершаются с депозитами на длительный срок) деньги ему возвращаются путем неоприходования средств, положенных на депозит другим клиентом (так называемая операция перекрытия).

Разновидностью сокрытия депозита может быть некоторое занижение в банковских документах реально внесенной суммы. Если занижение суммы незначительно, срок и проценты достаточно велики, а клиент не любит проверять правильность исчисления полученного дохода, то может даже не возникнуть необходимость в компенсировании ранее взятого депозита, так как «набежавшие» проценты замаскируют воровство.

Возможно и списание средств со счетов клиента. Если бухгалтер ленив и невнимательно следит за движением денег на счете своего предприятия, деньги могут списываться на третью фирму. Если клиент обнаружил списание — мошенник перед ним извиняется и деньги возвращаются. Если клиент ничего не заметил — доход получен.

Реально и перечисление денег от имени банка. Деньги снимаются не с расчетного счета клиента, а делается платеж от имени банка на какую-нибудь фирму, например, «на покупку компьютера», «за консультационные услуги» и т. д. при отсутствии (или фабрикации) подтверждающих документов.

Хотя подсовывание фальшивых долларов, немецких марок случается довольно часто (особенно в обменных пунктах), кассиры крупных банков предпочитают рисковать реже. Основная их «шалость» в этом плане — всучивание вместо новых купюр старых и потрепанных, которые трудно реализовать за полный номинал. Бывали случаи, что ранее выданные купюры те же кассиры через некоторое время принимали у клиента, отчаявшегося их реализовать, за часть номинала. Затем эти купюры снова всовывались в пачку невнимательному клиенту, и история повторялась.

Если клиент получает достаточно крупную сумму денег, то в банке у него часто нет возможности пересчитывать каждую пачку. Деньги без подсчета увозятся из банка и только у себя в офисе клиент их пересчитывает. Обнаруживается недостача, на которую кассир банка реагирует с олимпийским спокойствием: «Нужно было пересчитывать в банке!». Если клиент обнаруживает недостачу в банке, то перед ним извиняются и выдают деньги правильно.

Всегда возможно списать недостачи на другие подразделения банка. При доступе работников кассово-расчетного центра к бухгалтерским документам, возникшая недостача часто списывается на другие подразделения банка, где недостача может обнаружиться лишь через определенный период времени. Задержка во времени позволяет запутать ситуацию.

Для того чтобы в кассово-расчетных центрах банков минимизировать возможность махинаций, необходимо:

- ➡ проводить частые необъявленные пересчеты наличных денег как в кассах, так и в хранилище;
- ➡ работа в кассе должна быть как можно меньше связана с бухгалтерскими банковскими операциями;

- ➔ работники кассы не должны заниматься оформлением депозитных договоров или выпиской депозитных сертификатов;
- ➔ только кассиры должны работать с наличными деньгами. Если к деньгам допущен проверяющий кассу ревизор или аудитор, то со стороны работников кассы за ним должен быть организован контроль;
- ➔ кассирам нельзя позволять заполнять документы за своего клиента. Если клиент малообразован или болен, помочь составить документы должен специальный работник, не связанный с расчетно-кассовым обслуживанием;
- ➔ все операции, проходящие через кассира, должны надлежащим образом идентифицироваться как прошедшие его операционную обработку. На всех запакованных деньгах следует ставить фамилию кассира и дату помещения денег в упаковку;
- ➔ недопустимо хранение сберегательной книжки клиента, его депозитного сертификата, его экземпляра договора депозита (даже по просьбе клиента) у работника расчетно-кассового центра;
- ➔ категорически запрещено оставлять большие суммы наличных денег на виду у посетителей или посторонних для кассы работников банка. Существует много уловок отвлечения кассира и «выуживания» денег;
- ➔ все отправления денежных средств должны проходить проверку должностным лицом с тем, чтобы фиктивные перемещения денежных средств не могли использоваться для операции «перекрытия»;
- ➔ недостачи или излишки, обнаруженные в кассе, должны немедленно отражаться в сводном бухгалтерском учете;
- ➔ жалобы клиента на расчетно-кассовый центр рассматриваются должностным лицом, непосредственно не связанным с работниками указанной структуры.

46. КРЕДИТ ПОД «ДУТЫЙ» ЗАЛОГ ИЛИ ПОРУЧИТЕЛЬСТВО

Специфика работы кредитных отделов (в крупных банках — кредитных управлений) дает значительные возможности для различных злоупотреблений.

Любимое занятие отечественных «кидал» — взять кредит и не отдавать его. При взятии кредита злоумышленники часто не имеют достаточного залога или поручительства, в связи с чем им необходимы доверительные отношения с персоналом кредитного отдела, если, конечно, они не имеют выхода на высшее руководство банка.

Нередки случаи, когда работники этого отдела помогали получить кредит сомнительному клиенту с получением комиссионных до 30 процентов будущего безвозвратного кредита.

Все залоги, предлагаемые в качестве обеспечения кредита, должны исследоваться ответственными за эту акцию лицами банка, непосредственно не связанными с работниками, выдающими кредит. Его цель — определение реальной стоимости залога как перед получением кредита, так и по мере погашения ссуды.

Необоснованны займы фирмам, в которых есть личная заинтересованность банковских работников. Нередки случаи, когда высшие должностные лица банка имеют акции или другой экономический интерес в коммерческих структурах. Более того, они часто сами или через подставных лиц входят в органы управления такими структурами. Естественно, что они заинтересованы в процветании своих коммерческих предприятий даже в ущерб банку. В результате «свои» предприятия часто получают кредит под льготный процент даже при отсутствии залога или поручителя.

Если кредит выдается по решению высших руководителей банка, все документы о его выдаче заполняются относительно правильно. Однако если кредит «своему» предприятию необходимо продлить руководителю банка среднего уровня, то используется метод замены первого листа кредитного договора, на котором указана сумма кредита, его срок, процентная ставка. Подписи же руководства банка стоят обычно на втором (не заменяемом) листе. Естественно, что возникают проблемы в связи с наличием сводной отчетности по кредитам, но на практике они вполне решаемы.

47. НЕПРАВОМЕРНОЕ ОСВОБОЖДЕНИЕ ЗАЛОГА

Банк может понести значительные убытки из-за освобождения залога под кредит.

В отечественной практике все осуществляется достаточно примитивно. Клиент, взявший кредит, на определенном этапе начинает понимать (если он это с самого начала не предвидел), что он не сможет вернуть полученную ссуду. В нормальных условиях он не имеет возможности получить обратно свой залог, который, по правилам не должен находиться в распоряжении клиента. Однако он иногда его слезно вымаливает на том основании, что он срочно нужен для работы.

В качестве залога одним отечественным клиентом было предоставлено несколько грузовых автомобилей МАЗ. Когда срок возврата кредита стал истекать и кредитный отдел начал волноваться, клиент пришел в банк и сообщил, что товар, продажей которого он рассчитывается за кредит, уже прибыл на Брестскую таможенную и уже растаможен, о чем показал соответствующие факсы. Осталось всего-ничего — вывезти товар в магазины. Но поскольку деньги у клиента на исходе, арендовать транспорт он не может. Поэтому он попросил вернуть на несколько дней заложенные автомобили и обещал, что затем все будет хорошо.

И хотя в банке знали простоту фальсификации факсовых сообщений, клиенту пошли навстречу, залог раскрыли. В результате кредитные деньги безвозвратно ушли за границу, а автомобили были проданы ничего не подозревающему покупателю.

Кстати, в зарубежной практике все делается «элегантнее». В одном американском банке брокер по торговле хлопком имел большую задолженность банку по векселям, гарантированным товарными квитанциями, покрывающими большое количество хлопка. Спад на рынке хлопка привел к тому, что банк воздерживался от реализации залога в надежде, что рыночная стоимость хлопка увеличится. Это должно было позволить погасить кредит. Между тем брокеру потребовались дополнительные средства, но его заявки на получение кредита были отклонены.

Для решения проблемы кассир банка без ведома совета директоров освободил должнику указанные выше товарные квитанции, покрывающие большое количество хлопка. Затем брокер составил переводные векселя на один из своих загородных офисов, присоединил к ним освобожденные товарные квитанции и предъявил их кассиру банка для учета.

Сумма, выплаченная при учете векселя, была помещена на счет брокера, который незамедлительно использовал капитал для уплаты по обязательствам временного характера. Впоследствии загородный офис брокера заплатил по переводному векселю и возвратил товарные квитанции кассиру банка, который заменил их в картотеке залоговых бумаг. Данная операция повторялась несколько раз, пока в конечном счете банковский контролер не обнаружил мошенничество.

48. ПОЛУЧЕНИЕ НА СЕБЯ НЕОБОСНОВАННО БОЛЬШОЙ СУММЫ КРЕДИТА

Большинство банков дают возможность своим работникам брать определенную сумму кредита на выгодных условиях. В отдельных случаях им открывается кредитная линия в пределах установленного лимита. Такие кредиты периодически просматриваются руководством банка и кредитными комитетами.

Тем не менее некоторые банковские должностные лица на практике умудряются получать необоснованно большую ссуду, не уведомляя о ней руководство банка (например, путем фиктивного распределения денег на несколько подчиненных работников банка).

Политика противодействия необоснованному получению банковских ссуд должна включать в себя следующие моменты:

- ➔ решения о выдаче кредитов принимаются только коллегиально на заседании кредитного комитета или аналогичного ему органа;
- ➔ четко разграничиваются полномочия руководителей различного ранга по выдаче кредита и установлению процентных ставок;
- ➔ все выданные или продленные кредиты полностью обеспечиваются ликвидным залогом, находящимся в распоряжении банка, или поручительствами (гарантиями). Осуществляется постоянный и тщательный контроль за наличием залога по ссудам;
- ➔ проводятся регулярные проверки правомерности выдачи кредитов и установления процентных ставок;
- ➔ жестко контролируется расходование средств со спецссудного счета клиента, взявшего кредит;
- ➔ назначаются незаинтересованные служащие для проверки обязательств по каждому заемщику.

Вексель является долговым документом, оформленным строго определенным образом с набором стандартных реквизитов. Для того чтобы вексель был признан недействительным, мошенники умышленно нарушают законодательно установленную процедуру оформления векселя.

В ряде случаев векселя выписывают подразделения или филиалы крупной хозяйственной структуры, которым головной офис такого разрешения не давал. В результате подобные векселя признаются недействительными. И в этом случае страдает клиент.

Один из крупных российских банков привлекал средства через свои филиалы путем выписки векселей от имени этих филиалов. Когда банк обанкротился и клиенты начали требовать свои деньги назад, выяснилось, что головное отделение банка не давало право своим филиалам эммитировать векселя. Через суды все векселя были признаны недействительными. Клиенты же не могли получить проценты по векселям. Поскольку сделки признавались недействительными, то клиенты могли рассчитывать на возврат только суммы, которую они перечислили в банк. Естественно, что они сильно теряли из-за инфляции. Более того, из-за банкротства банка и эту сумму многие займодатели не смогли вернуть.

49. ЗЛОУПОТРЕБЛЕНИЯ ПРИ КОНВЕРТАЦИИ ВАЛЮТ

Конвертация валюты — весьма распространенная операция в банках Балтии для клиентов из Беларуси, России, Украины и некоторых других стран, где существует достаточно жесткое валютное регулирование.

Такая конвертация обычно производится через офшорные компании, курс согласовывается по телефону. Если реальный курс оказывается для клиента менее выгодным по сравнению с согласованным по телефону, он тем не менее вынужден соглашаться. Это создает возможности для злоупотреблений со стороны работника банка, занимающегося конвертацией.

Клиенту работник банка может даже прислать факс о курсе конвертации валюты. Но сегодня факсы не подделывает только самый ленивый.

Как известно, компьютер может делать валюту «из воздуха». В условиях постоянного и динамичного изменения курса валют открываются дополнительные возможности для махинаций. Они основаны на неправильном пересчете курсов валют. Такую неправильность аферисты могут заложить прямо в компьютерную программу.

В одном из ведущих московских банков начальник отдела автоматизации неторговых операций модернизировал компьютерную программу учета движения валютных средств банка по счетам граждан. В результате эта программа при введении коммерческого курса рубля зависила на 700 тысяч долларов курсовую разницу, предназначенную для зачисления на счета граждан.

Эту разницу нужно было «разбросать» по счетам. С этой целью на 121 банковский счет граждан были перечислены суммы от 4 до 6 тысяч долларов. При этом использовались счета владельцев, имеющих незначительные остатки (от нескольких центов до 10 долларов), и обращение которых в банк было маловероятно. Поскольку таких счетов оказалось недостаточно, то мошенник был вынужден восстанавливать уже закрытые счета, а также открывать новые. Естественно, что юридические дела на вновь открываемые счета отсутствовали, а на закрытые счета дела были уже в архиве.

Оставалось «вытащить» расписанную по счетам валюту. Компьютерная программа и здесь оказала помощь. Путем ее очередной модернизации все деньги были перераспределены на открытые сообщником счета.

Последний воспользовался шестью украденными или потерянными паспортами других граждан, в которые вклеил свои фотографии. Он предъявлял эти паспорта в банке и спокойно снимал деньги. Похищенная валюта делилась с начальником отдела автоматизации.

Если на одном бланке несколько переводов, то необходимо проверять сложение обоих видов валют, так как были случаи мошенничества, когда преднамеренно осуществлялось неправильное сложение. С целью предупреждения хищений валюты, полученной по почте, рекомендуется всю поступающую иностранную почту вскрывать в присутствии двух лиц. Валюта должна пересчитываться одним работником, а проверяться другим.

Иногда происходит хищение средств, полученных для переводов. Афера состоит в переводе лишь части предназначенной для перевода суммы. При «наглom» хищении перевод вообще может не делаться. Если обязанности кассира состоят и в приеме денег, и в оформлении перевода, то хищение обнаружить достаточно сложно.

Однако они достаточно легко выявляются при поступлении из-за границы жалоб на то, что денежные переводы не поступили или их сумма оказалась меньше ожидаемой.

Наряду со стандартными предложениями типа «крепить учет и контроль» можно рекомендовать следующие эффективные меры:

- ➔ конвертации иностранных валют должны осуществляться одним лицом, а проверяться другим;
- ➔ обязанности работников должны разделяться для того, чтобы осуществление афер было возможным только при наличии сговора. Совершить мошенническую сделку на основе сговора вдвоем сложнее, чем в одиночку, а втроем сложнее, чем вдвоем;
- ➔ по мере возможности вся поступающая почта, особенно почта из-за рубежа, должна вскрываться в присутствии двух лиц;
- ➔ комиссионные сборы за осуществление валютных операций должны регулярно проверяться на предмет правильности инкассации и правильности осуществления проводок;
- ➔ оплата дорожных чеков должна проводиться не тем лицом, которые эти чеки выписывает.

50. ЛЖЕБАНКИР И «ЛЖЕПАНАСОНИК»

Главным организатором и идейным вдохновителем этой аферы был российский гражданин, бывший банкир, который и придумал новую схему честного облапошивания.

Изобретенная мошенником схема, в результате реализации которой различные фирмы из многих регионов России лишились миллиардов неденоминированных рублей, вполне могла бы претендовать на какую-нибудь премию по экономике, если бы ее претворение не завершилось столь плачевно. Тем более что ее масштаб вполне сравним с аферами начала 90-х годов XX века по поддельным чекам России и пресловутым авизо.

Сначала преступники покупали какой-нибудь терпящий бедствие небольшой московский банк, у которого к тому времени Главное управление ЦБ РФ отозвало лицензию на проведение некоторых операций и даже вообще лишило лицензии.

А затем, получив право управления, назначив своих людей на руководящие должности и законно завладев печатями, штампами и прочими официальными банковскими атрибутами, преступники, действуя силой или за деньги, выкупали у прежнего руководства чистые бланки векселей, которые тоже на тот момент еще были настоящими, но уже неликвидными. Заполнив векселя, лжебанкиры иногда через посредников или прямо по факсу направляли свое предложение различным коммерческим фирмам, у которых, по их

сведениям, были значительные долги перед федеральным и местным бюджетом, свои предложения помочь рассчитаться с государством.

Ничего не подозревавшие коммерсанты приезжали в Москву, в солидный банк, где их встречали прилично одетые люди, утверждавшие, что они честные банкиры. Коммерсанты рассчитывались каким-нибудь имеющимся у них в избытке товаром на обозначенную в векселе сумму через опять-таки подставные фирмы и получали платежное поручение и заверения, что все их долги будут перечислены банком государству. Развязка, как правило, наступала через несколько месяцев. К тому времени, разумеется, найти концы обманутые предприниматели самостоятельно, естественно, не могли.

Отечественные бизнесмены часто весьма наивны при осуществлении международных сделок, часто верят дутым гарантиям и письмам, подтверждающим солидность зарубежной фирмы.

В мировой практике распространена подделка документов следующих банков: «Standby Letters of Credit», «Bonus Loan Forms», «Prime Bank Discounted Letters Credit», «Zero Coupon Letters» и др. Иногда мошенники используют названия организаций, сходных по звучанию со всемирно известными банками и фирмами. Они и сами могут создать такие названия, заменив одну-две буквы.

Имея дело с фирмами «Panasonic», «Panassonic», «Panasonik», некоторые наши коммерсанты были сначала искренне уверены, что они покупают продукцию всемирно известной компании «Panasonic». Потом они разобрались, но тем не менее продолжают надувать население, продавая за «фирму» подделки с измененной в названии производителя буквой.

Мошенники могут выступать и от имени дочернего предприятия известной зарубежной фирмы. Для этого достаточно выдумать громкое имя и зарегистрировать под этим именем фирму.

Она может носить, например, название «Бош Белорашн», «Диор Интернешнл». Если регистрирующий орган вдруг воспротивится использованию названий известных фирм, то выход прост: название регистрируется в виде аббревиатуры, которое расшифровывается во внутрифирменных и фальсифицированных документах. Для поднятия своего престижа эти документы предоставляются клиентам на просмотр.

В результате клиентов не удивляет, если в платежных поручениях на перечисление денег их попросят указать просто: «АБМ, региональное отделение».

После официальной регистрации фирмы злоумышленники фабрикуют документы, свидетельствующие об их родственных отношениях со знаменитой фирмой, выступающей гарантом их операций.

Практика показывает, что не все клиенты достаточно до-тошны и внимательно изучают предоставляемые документы, а тем более обращаются в регистрирующие органы или в соответствующие инстанции для выяснения дополнительных подробностей. Выяснения обычно начинаются после того, как клиент уже пострадал от мошенников.

Подобные аферы обычно совершают лица, которые действительно работали или работают в зарубежных представительствах на второстепенных должностях, но имеют доступ к некоторым внутрифирменным документам. На основе таких документов они делают достаточно качественные подделки. Кроме того, в представительствах можно обзавестись каталогами и заключать от их имени договоры с условием, что договор должна будет исполнять известная компания, а деньги будут направляться на счет мошеннической фирмы.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	3
ГЛАВА 1. ИРПИЧ, КАК ИЗВЕСТНО, НИКОГДА НИ С ТОГО НИ С СЕГО НА ГОЛОВУ НЕ ПАДАЕТ	8
1. ОПЛАТА БУДУЩЕГО «ТРУДОУСТРОЙСТВА»	8
2. БАБЕТТА ИДЕТ НА «СОБЕСЕДОВАНИЕ»	10
3. КУРСЫ ДЛЯ ЖЕЛАЮЩИХ «НАЧАТЬ НОВУЮ ЖИЗНЬ»	11
4. ХОТИТЕ НАУЧИТЬСЯ БРИТЬ ПОДМЫШКИ?	12
5. КУПИТЕ ОТКРЫТКУ ДЛЯ ДЕТЕЙ-СИРОТ	13
6. ОБОРУДОВАНИЕ ДЛЯ ПРОСМОТРА КАБЕЛЬНОГО ТЕЛЕВИДЕНИЯ	14
7. ЛОТЕРЕЙНЫЙ «ЛОХОТРОН»	14
8. «ЖАДНОСТЬ ФРАЕРА СГУБИЛА»	15
ГЛАВА 2. «МОБИЛКИ» ДЛЯ ЛОХОВ, ИЛИ КАК ТЕЛЕФОН В РУКАХ ПРЕВРАЩАЕТ ЧЕЛОВЕКА В ОБЕЗЬЯНУ	17
9. «ДЕТИ ЛЕЙТЕНАНТА ШМИДТА»	17
10. КЛОНИРОВАНИЕ ТЕРМИНАЛОВ	18
11. БЕСПЛАТНЫЕ ТЕЛЕФОННЫЕ ЗВОНКИ ОТ ОПЕРАТОРА «ЛОХ-GSM»	21
12. МОШЕННИЧЕСТВА С ТЕЛЕФОННЫМИ КАРТАМИ	23
13. МГНОВЕННАЯ УСТАНОВКА ДОМАШНИХ ТЕЛЕФОНОВ	23
ГЛАВА 3. КВАРТИРНЫЙ ВОПРОС, КОТОРЫЙ ЗДОРОВО ИСПОРТИЛ ЖИЗНЬ МНОГИМ ЛЮДЯМ	24
14. «НЕХОРОШАЯ» КВАРТИРА	25
15. «КОТ» В КВАРТИРЕ	27
16. ПОДДЕЛКА ДОКУМЕНТОВ В МОМЕНТ КУПЛИ-ПРОДАЖИ ЖИЛЬЯ	27
17. ПРОДАЖА КВАРТИРЫ «ПОД ПРИНУЖДЕНИЕМ»	29
18. АГЕНТЫ-МОШЕННИКИ	30
ГЛАВА 4. ТУРИСТ — ИДИОТ ПО ОПРЕДЕЛЕНИЮ?	31
19. АГЕНТСТВО И «АГЕНТСТВОЧКО»	32
20. МОШЕННИЧЕСТВА В ХРАНИЛИЩАХ БАНКОВ	34
21. БИЛЕТИК ВНЕ ОЧЕРЕДИ	35
ГЛАВА 5. ВЫЙТИ УДАЧНО ЗАМУЖ	36
22. ЖЕНЩИНА ДЛЯ «ФРАНЦУЗСКОГО ЛЕЙТЕНАНТА»	37
ГЛАВА 6. АВТО-БЕНДЕРЫ И АВТОЛОХИ	38
23. «МЕРТВЫЕ ДУШИ» И ЖИВЫЕ МАШИНЫ	39
24. «СЕРЫЕ АВТОМОБИЛИ»	39

ГЛАВА 7. ПИРАМИДЫ ЕГИПЕТСКИЕ И ФИНАНСОВЫЕ	41
25. КАК ПОПАСТЬ В «ПИРАМИДУ»?	43
26. ПЛАТА ЗА «ЭЛИТАРНОСТЬ»	44
27. «ИНВЕСТИЦИОННАЯ» ДЕЯТЕЛЬНОСТЬ	46
28. ПРОДАЖА «УСЛУГ»	47
29. КЛУБ «ЕДИНОМЫШЛЕННИКОВ» В ИНТЕРНЕТЕ	48
30. КАК СТРАХУЮТСЯ «СФИНКСЫ», СТЕРЕГУЩИЕ ПИРАМИДЫ?	49
ГЛАВА 8. КРЕДИТНЫЕ КАРТОЧКИ, ЭЛЕКТРОННЫЕ ПЛАТЕЖИ И ИНТЕРНЕТ	50
31. КРАЖА ПЕРСОНАЛЬНЫХ ДАННЫХ ВЛАДЕЛЬЦЕВ ПЛАСТИКОВЫХ КАРТОЧЕК	50
32. ОПЕРАЦИИ С ПОДДЕЛЬНЫМИ КАРТАМИ	53
33. ОПЕРАЦИИ С УКРАДЕННЫМИ ИЛИ УТЕРЯННЫМИ КАРТОЧКАМИ	55
34. МОШЕННИЧЕСТВО С ПОЧТОВЫМИ И ТЕЛЕФОННЫМИ ЗАКАЗАМИ	58
35. АФЕРЫ С ИСПОЛЬЗОВАНИЕМ ПОДЛОЖНЫХ СЛИПОВ	60
36. МАХИНАЦИИ С БАНКОМАТАМИ	61
37. АФЕРЫ В СЕТИ С КАРТАМИ И БЕЗ ОНЫХ	66
38. МОШЕННИЧЕСКИЕ ESCROW-УСЛУГИ	71
ГЛАВА 9. ИНВЕСТИЦИОННЫЕ АВАНТЮРЫ В СЕТИ ИНТЕРНЕТ	72
39. «ПИСЬМА ИЗ НИГЕРИИ»	72
40. «НАДУВАНИЕ ПУЗЫРЯ»	74
41. НАВЯЗЫВАНИЕ ИНФОРМАЦИИ	76
42. ГЕНЕРАЦИЯ ТИТУЛЬНЫХ ЗНАКОВ WEBMONEY (WM)	79
ГЛАВА 10. МАХИНАЦИИ С БАНКОВСКИМИ ОПЕРАЦИЯМИ	80
43. МАХИНАЦИИ С ПРОСТЫМИ ВЕКСЕЛЯМИ	81
44. ОТЗЫВНЫЕ ДЕПОЗИТНЫЕ СЕРТИФИКАТЫ	82
45. РАСЧЕТНО-КАССОВОЕ ОБСЛУЖИВАНИЕ	83
46. КРЕДИТ ПОД «ДУТЫЙ» ЗАЛОГ ИЛИ ПОРУЧИТЕЛЬСТВО	85
47. НЕПРАВОМЕРНОЕ ОСВОБОЖДЕНИЕ ЗАЛОГА	86
48. ПОЛУЧЕНИЕ НА СЕБЯ НЕОБОСНОВАННО БОЛЬШОЙ СУММЫ КРЕДИТА	88
49. ЗЛОУПОТРЕБЛЕНИЯ ПРИ КОНВЕРТАЦИИ ВАЛЮТ	89
50. ЛЖЕБАНКИР И «ЛЖЕПАНАСОНИК»	91

Справочное издание

**50 СПОСОБОВ ОТЪЁМА ДЕНЕГ
СОВРЕМЕННОГО ОСТАПА БЕНДЕРА**

Автор-составитель *СМИРНОВА Любовь*

Ответственный за выпуск *М. В. Адамчик*

Подписано в печать с готовых диапозитивов 18.01.06.
Формат 84×108¹/₃₂. Бумага газетная. Печать офсетная.
Усл. печ. л. 5,04. Тираж 5100 экз. Заказ 199.

Издательский кооператив «Современный литератор».
Лицензия № 02330/0133053 от 30.04.04.
РБ, 220029, Минск, ул. Киселева, 47, к. 4.

При участии ООО «Харвест». Лицензия № 02330/0056935 от 30.04.04.
РБ, 220013, Минск, ул. Кульман, д. 1, корп. 3, эт. 4, к. 42.

Республиканское унитарное предприятие
«Издательство «Белорусский Дом печати».
220013, г. Минск, пр. Независимости, 79