New Technology Briefing

E-commerce and identity fraud

Gareth Jones
is an ex-Fraud Squad and SFO detective and head of fraud at Experian.

Gareth Jones

Received (in revised form): 19 December 2000

Abstract
This paper focuses on the subject of personal and corporate identity in the UK, the ways in which identity can be substantiated, and the methods used by fraudsters to invent identities or copy other people's identities. The setting for this is the Internet, as utilised as a channel of introduction by two market sectors — retail and financial services. The paper considers the availability and suitability of deploying fraud prevention solutions to reduce substantiated fraud and discourage repeat attacks.

Keywords: identity, validity, verification, identity fraud, impersonation, transaction fraud

Introduction

The sensitivity surrounding companies' real exposure to fraud perpetrated through the Internet is such that this paper makes no reference to specific organisations by name. It will, however, cover what fraud goes on and why, and reflect on how these crimes can be prevented and the consequent impact of doing so.

To give this paper some context, it is appropriate to start with the most recent figures on domestic Internet usage. These are drawn from a survey of over half a million Internet users conducted as a part of Experian's Canvasse Lifestyle survey questionnaire, which was completed in December 2000.[1] It represents the most statistically valid analysis of actual consumer Internet usage in the UK, and provides a powerful insight into changing Internet shopping patterns over the last 12 months, as well as a breakdown of the age, income, purchasing frequency and types of products purchased by online shoppers. The figures show that the number of people purchasing on the Internet has more than doubled since the beginning of the year. The survey reveals that people are starting to buy more frequently on the Internet, with 1.45 million consumers making four or more purchases since January 2000: the most popular items are holidays, books, computer games and music.

Internet purchasing: Canvase Lifestyle survey results reveals increased purchasing

The key findings from Experian's Canvasse Internet survey are as follows.

— The proportion of the UK population purchasing over the Web in the last 12 months has more than doubled, from 5.1 per cent (2.26 million adults) at the beginning of 2000 to 10.7 per cent (4.7 million adults) by December 2000.
— Some 3.3 per cent of the UK adult population — around 1.45 million people — had made four or more purchases online since the start of the year. At the same time, the proportion of adults who bought online

Gareth Jones
Head of Fraud,
Experian,
Talbot House,
Talbot Street,
Nottingham NG1 5HF,
UK
Tel: 44 (0) 115 976 8901
E-mail:
gareth.jones@UK.experian.com

just once in the same period decreased from 35 per cent to 27 per cent, but the proportion purchasing four or more times in the same period increased by over a quarter from 24 per cent to 31 per cent. This suggests that people are starting to purchase online more frequently.

Most popular online purchases: holidays, books, computer games, music

— Holidays, books, computer games and music remain the most popular purchases, and each of these categories is increasing as a proportion of online purchases. Holiday purchasing is up a fifth from 14 per cent to 17 per cent of online purchases. This growth may well be due to increasing transparency and availability of last-minute/discount bookings services from airlines and tour operators, supported by serious above-the-line campaigns in broadcast and print media as well as online advertising (Table 1).

— Internet shoppers are mainly younger and wealthier people (Tables 2 and 3). Measured against the national norm, the age group most overrepresented among online shoppers is 18–25 year olds (more than double the national average). However, a significant number of online shoppers are in the 26–45 age bracket; 26–35 year olds are overrepresented at almost 166 per cent of the national norm, whereas 36–45 year olds are a fifth up on the national average. The survey

Table 1: Internet shopping by products

	January 2000 (%)	December 2000 (%)
Books	28	29
Music	18	21
Holidays	14	17
Computer games	12	12
Video	6	7
Fashion wear	8	6
Wine	3	3
Children's clothes	2	2
Garden	3	2
Financial	4	1
Health	3	1

Table 2: Internet shoppers — Income split

	Internet shoppers (%)	UK average (%)
£0–19,000 pa	33	65
£20,000–39,000 pa	42	27
£40,000–60,000 pa	16	6
Over £60,000 pa	9	2

Table 3: Internet shoppers — Age split

Online shoppers age profile: dominated by 18–25 year olds

	Internet shoppers (%)	UK average (%)
18–25	9	4
26–35	27	17
36–45	25	20
46–55	19	18
Over 55	20	41

also reveals significant purchasing activity from the over-55 age bracket (known as 'Silver Surfers'). Although this represents half the national norm as a proportion of the online purchaser community, Silver Surfers now conduct a fifth of all online purchases.

— A significant percentage of online shoppers do not consider the Internet a valuable educational resource (37 per cent), while just 22 per cent said that it was valuable. The remainder (41 per cent) were neutral on this question.

Internet usage: More than doubled in last 12 months

The Canvasse Lifestyle results also enable us to assess the actual size of the Internet market, and how this market has grown over the last year. Based on the assumption that the average Internet purchase is around £50, we can estimate that Internet sales have more than doubled over the past year, growing from £264m at the start of January 2000 to an annualised £602m by December 2000.

Online consumer transactions largely fraud free

These figures tend to suggest that the consumer is not overly concerned about the risk of fraud, albeit perusal of recent articles on e-commerce fraud would leave the public with the perception that the Internet is a lawless zone where only the confident should tread. This of course is nonsense to a well-travelled and Web-wise surfer; providing that even newcomers install virus guards, and have an awareness of their rights and exposure to liability under the terms of agreements with their financial services suppliers, then the Web is a relatively safe and fun place to interact. In short, transactions with eBusinesses are nearly always free of fraud risk to the consumer (see section 'Business Identity Fraud'). However, trading with customers over the Internet is a very different kettle of fish, or rather sharks. There are a multitude of ways in which businesses can be defrauded, and in the same breath, plenty of ways in which such crimes could be prevented. Ultimately the ratio between risk and its actualisation varies depending on the skill-set of current and potential offenders, and the measures taken by a range of potential victims to protect themselves.

The remainder of this paper is rather like *The Bill* meets *University Challenge*. The 'starter for ten' is to consider what identity is, and whether it matters on the Web; if so why; if not, what are the alternatives? Next get into the sexy territory of *The Bill*, and consider how fraud happens, the *modus operandi*, from both a consumer and business perspective. After this lesson in how to do it, any reader thinking of a more nefarious change of career is advised to digest the fraud prevention solutions section first, otherwise their grand scheme may be rather short-lived! Finally, there is a section that rounds up the privacy issues, which any paper on identity and fraud should touch upon. All of this is referenced to two market sectors, e-tail and financial services, for no particular reason other than that is where it is all happening!

What is identity?

Identity is not just our full name. It is much more than that. It extends to who we were (in the event of a change of name), our date and place of birth, our address, and even coded references to ourselves. Indeed, to

certain organisations we are more accurately identified by numbers and coded references than by our name and residence. Different organisations take a different view on what characteristics taken together comprise identity, and in the financial services sector this is mandated by regulation. Beyond the UK, identity characteristics vary from country to country. So it is not as straightforward as one might imagine.

Absence of national identity card complicates the process of customer identification

This is because the UK differs from many other countries in not having a national identity card. The consequence of such a device's absence is that our identities can only be objectively assessed by accessing a range of materials in which the identity is referenced, and an amalgamation of which is persuasive in proving who we are. Proof of identity is therefore drawn compendium style as extracts from a reference platform of paper records and data events, none of which has the sole function of proving who we are but, taken as a whole, can be compelling in establishing this.

And this, in short, is the seat of the problem. The aim of identification is to be absolutely reassured that the customer is who they purport to be, but the reality is that confidence in this outcome will vary from one person to another according to whether their identities are both recorded and accessible in the reference platform. Thus the real issue is the capability of the methods by which businesses can calculate the measure of confidence they can have in the customer's identity, bearing in mind that not all customers are alike.

Fraudsters don't usually know their victims details

The reliability of the confidence assessment will be supported or attenuated by the ability of businesses to capture or ask for those personal characteristics of customers that are useful in confirming identity. This is relevant because impostors — those who pretend to be someone else — are very often exposed by failing to mimic accurately the 'lower-level' identity characteristics of the real person — such as their correct previous address, their work telephone number, the length of time they have lived at their address, and often their date of birth. Neither will they know more intimate information, such as the numbers or details of financial services accounts opened by the real person being impersonated.

Validity verification identification

With all these caveats in mind, the assessment of identity is founded in satisfying two criteria: 'validity' and 'verification'. The first step is to ensure that the individual exists, the second is to link the applicant to the identity. In calculating whether these two criteria have been satisfied, it is necessary to factor in risks surrounding the issue of the reference material. It is appropriate to consider the enrolment methods of both public and commercial sector organisations from which the material originates, its exposure to fraud and forgery, and whether there is some form of positive linkage to the individual presenting it.

Clearly, as consumers, we can expect these processes to be proportionate to the purpose of the identification. We do not expect to be as thoroughly identified when conducting a simple purchase transaction as, say, when opening a new financial services facility. Business assessment of a customer's identity matters, because whereas transactions may be initially authorised, false identities invariably lead to 'chargebacks' and losses will be incurred by the retailer. In the provision of financial services, false identities need to be detected for two reasons:

diligence in the prevention of fraud (which invariably causes losses), and compliance in the prevention of money laundering. Thus the level of confidence businesses choose to have in the assessment of their customer's identities will vary from one market sector to another.

Leaving consumer identification for a moment, most businesses have their own identity too. Anyone who has studied law will recollect the case *Solomon v Solomon*,[2] which ruled that incorporated businesses have a legal personality distinct from those of their officers and members. Smaller businesses such as partnerships and sole traders do not have a separate legal identity to their proprietors, and therefore such small organisations are considered for legal purposes to be persons. For the provision of business-related financial services, organisations are identified at a personal level, typically by checking the identity of directors. Thus business and consumer identities are in effect measured in the same way.

Businesses have their own identity

So why does identity matter? What are we getting hung up about? It matters because it is the unique key to referencing our status, qualifications, rights and privileges that have been awarded to or earned by us. It is these things taken together that make us unique, and consequently enable subjective evaluations of our performance, propensities, profession, capabilities, interests and ultimately our worth and value. Consequently, our identity is one of our most valuable possessions, and attacks upon its credibility by fraudsters are taken personally and hurtful to us. In the event of it happening, it feels like a kind of criminal defamation of our character, and it matters less what has been done in our names than who it is people think did it. Avoidance of blame is uppermost in an identity fraud victim's mind. Victims care that they are distinguished from 'suspects', and it is therefore a 'given' that those storing identity data do so responsibly, and protect people from attack, abuse and fraud. This is also a legal requirement under the Data Protection Act 1998.

Identity is one of our most valuable posessions

The true identity of dot.com businesses' customers matters because their worth as a going concern is scaleable according the size and integrity of their customer base. It is from this so-called 'jewel in the dot.com crown' — their databases of customers — that the opportunity to segment, market and cross-sell is leveraged, and therefore the level of confidence they have in their customers' identities is of great importance.

The identity of a business is just as crucial, because attached to its name is the subjective level of confidence a customer places in the organisation's integrity, plus the quality of product and service. It is common to replace this subjective level of confidence with an objective one supplied by a third party. To bring about consumer confidence in new and existing companies trading on the Web, 'seal' schemes have been promoted to verify the integrity of the organisation behind the Web page. Obtaining business information on the organisation and its directors is another way of accessing data that support the company's credibility and enhance trust.

Business information supports dot.com credibility

Both consumer and business identities can be copied or falsified. Whereas the level of this varies between market sectors, it is a significant problem and one that deserves some explanation. Knowing how it

happens allows us to set in place procedures that detect and prevent the outcome, which manifests itself in losses. It also enables us to consider what measure of fraud prevention diligence we can stand against the likely reaction to this of 'good' customers, and the operational cost burden of bothering to identify them in the first place. This is especially important in the retailing sector, where minimum standards are not dictated through regulation and non-transparent procedures could disaffect good customers at the cost of sales.

There are occasions when the disclosure of true identity is not the norm. This is the case in a variety of real- and virtual-world environments. In the real world, identity is not an issue in a cash transaction, so why expose it? In the virtual world it is the norm to use a 'nickname' in chatrooms. Whereas this is unlikely ever to change, it has its dangers, as the anonymous nature of this environment allows those with certain persuasions to present an untrue picture of themselves. The danger of this is borne out in the many reports of paedophiles using these environments to 'groom' unwitting children and adolescents into meetings.

Dangers of anonymity all too apparent

Methods of committing fraud

The extent of exposure of good business to deceit perpetrated by fraudsters varies from retailing to financial services. Generally it is a single-figure percentage of volumes, though it can be far higher in certain markets. In both e-tailing and financial service sectors there is a wealth of evidence of organised crime, where those culpable pursue other criminal practices, including the sale of pornography and drug trafficking. Thus fraudsters should be regarded first and foremost as criminals who are presently committing fraud, as they are often undeserving of the 'white-collar' label so frequently generically applied to their types.

Fraudsters often undeserving of 'white collar' status

It is not possible to detail comprehensively all the methods of committing identity fraud, but the main ones can be sufficiently covered. Because of the diverse nature of fraud across retail and financial services markets, it is appropriate to divide the methodology by sector, first taking transaction fraud against business, then financial services and identity fraud, and finally business identity fraud.

Transaction fraud

This is the process of duping retailers into accepting that the fraudster has the rights to use a payment card — credit or debit. The fraudster chooses whether to use the name of the cardholder, a third party's name or an entirely false name, depending on their access to information about the real cardholder, access to premises to receive the goods, and their general level of proficiency in exercising the scam. A recent survey by Experian[3] revealed that fraudsters have realised that methods of prevention are currently so inadequate they need spend little time or effort covering their tracks. Less than 10 per cent of fraudsters bother with a redirection service at the goods delivery address, and only 10 per cent make the effort to set up a false telephone account.

Experian survey: fraudsters are often unsophisticated

In order of prevalence, the most common methods of conducting transaction fraud were revealed as follows:

— using a real name at a real address but not the cardholder's name
— using the cardholder's name at a real address but not the cardholder's address
— using a false name at real address
— using the cardholder's genuine name and address but goods delivered to another address.

Thus the survey revealed that one of most common features of CNP (card not present) fraud is 'real name at a real address but not the cardholder's name' (and address). In other words, the fraudster had a real person's name that was or had been in the past associated with a genuine address, but the card number given matched a different name and address. This suggests inadequate procedures for identifying real people from imposters, and endorses the requirement to link the card number to the genuine cardholder's address.

More work needed to identify the customer

The next most common — 'cardholder's name at real address but not cardholder's address' — suggests that fraudsters are giving names to match the card account name but the address provided does not match the billing address. This again supports the need for linkage between the card number and the cardholder's billing address.

'False name at real address' was also a common tactic, but this could only work where retailers did not check to see if the customer was referenced on various data sources. This lack of checking is borne out by other findings in the research and could easily be prevented.

Finally, 'cardholder's genuine name and address but parcel delivered to another address' illustrates a dilemma faced by online retailers in dispatching goods to addresses other than the cardholder's billing address. In many cases, as in the case of presents, etc, these transactions will be genuine, but the process clearly lends itself to extensive abuse by fraudsters and is an easy way to defraud an online retailer. With the introduction of the card issuers' address verification system (AVS) (which correlates the card number to the billing address of the cardholder at the point of authorisation), through crime deflection this method could well become the preferred choice for fraudsters conducting remote transactions.

New industry initiative will be effective to a point

Despite the relative ease of obtaining credit card numbers from discarded till receipts, credit card statements in domestic waste bins, collusion within retailer operations and credit-card-number-generating software, it is more difficult to get the correct name and address of the cardholder, and the expiry date of the card also needs to be established. However, once the expiry date for one card number has been ascertained, fraudsters realise that other card numbers that are sequential to it may have the same expiry date, extending their arsenal of valid data to commit fraud.

The tools of the fraudsters trade: Credit card number generating software

Credit-card-number-generating software, such as that pictured in Figure 1 — freely available on the Internet — is the root cause of much of the card-not-present transaction fraud problem. Indeed, the ability of Web users to present themselves anonymously to user groups and websites promotes promiscuity in the area of identity, and it is not difficult to

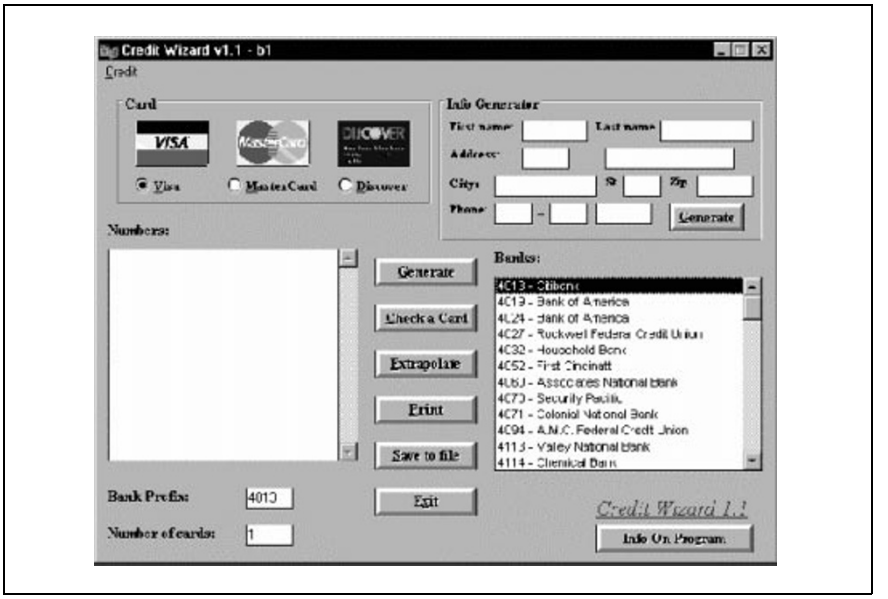

Figure 1: Example of a software program that generates credit card numbers

obtain forged evidential proofs of identity through this channel (see phatism.com or search for 'café covert' as examples of this).

Industry initiatives will raise fraudster's game

But with AVS and other solutions in place in the future, the fraudster will have to be cleverer, establishing at least the correct address for the cardholder or, once they understand how AVS works, giving postal addresses with the same numerical values, practising account takeover, or using third-party delivery addresses to receive the goods. Virtual goods and services will not be so problematic, as if they know the correct address for the cardholder fraudsters can impersonate them with confidence, as the 'goods' are virtual, and the connection between computer IP addresses and physical real-world addresses can be masked.

Other ways of establishing bona fide cardholder details include hacking into websites (remember the CD Universe case) to obtain both customer and card data. This allows exact impersonations to be conducted with relative ease. The impact of these attacks is severe on both the primary and incidental victims. The primary victim — the genuine cardholder — has a tendency to lose confidence in the card and reduce their spending upon it. However, they are protected under the terms of the Consumer Credit Act and invariably suffer no financial loss. The e-tailer whose site has been hacked risks customer defection *en masse*, affecting the viability of their future Internet trading; and the card issuers suffer the operational burden of administering the fall-out of the compromise in the form of reissuing plastic, subsequent chargebacks, and loss of revenue from interchange fees because of reduced card usage.

Plastic no longer fantastic – loss of confidence

Financial services and identity fraud

The fraudulent obtaining of financial services (application fraud) requires greater research by the criminal, though the rewards can be higher than with transaction fraud. The target products for offences of impersonation

Cash and consumer goods are favourite target

and false identity tend to be those that allow the fraudster to acquire cash or goods. The favourites are all forms of credit — retail or cards, loans and asset finance agreements. This is because the goods obtained are either cash, domestically desirable items that can be traded for cash, or goods that can be converted for a high price — such as cars and motorbikes.

So how is identity fraud perpetrated? The methods are numerous, but broadly speaking fall into two categories. There are impersonations, where the fraudster adopts the identity of another person — real or deceased. The other method is to create or 'grow' an identity as if it were real. The following describes at a relatively high level how these offences are committed, but not in sufficient detail to provide a 'blueprint' to a tempted reader!

Impersonations

There are three types, with many variations on the themes presented here:

— 'current address impersonation'
— 'previous address impersonation'
— 'deceased impersonation'.

Data sharing is key to exposing fraud

'Current address impersonation' is where the fraudster copies the identity of a real person who is, or was, the occupier of the address they describe on the application form as being their 'current address'. The fraudster will accurately replicate the high-level characteristics of their 'victim' — typically name and address — but is often unable to establish lower-level detail, such as date of birth, time at address, previous address, and other biographical details such as employment information. This allows those lending organisations that are members of data-sharing systems to develop rules that expose these low-level inconsistencies, and detect the fraud.

'Previous address impersonation' is more common. Here the fraudster copies the identity of a person who is still resident at the address quoted on the application form as the 'previous address'. They will of course give a 'current address', but state that they have only lived there for a short period of time. The details of credit recorded in the victim's name (at the previous address) are then pulled through, and the fraudster 'adopts' these to demonstrate creditworthiness.

'Jackal' fraud still common

'Deceased impersonation' is rare, but when practised it can be effective. It is the style of deceit that Frederick Forsyth wrote about in *The Day of the Jackal*, involving the copying of a deceased person's identity. The deceased is very often a child who was born in the same era as the imposter. This information is often obtained from graveyards. The fraudster will then obtain a birth certificate in the child's name, and use this document to apply for others — such as a passport or driving licence. Birth certificates are aptly termed 'breeder documents', because they can be used to generate other proofs. Where the deceased victim was an adult at death, the fraudster has the benefit of acquiring their biographical identity features, but rarely uses their date of birth if they were elderly

and the fraudster much younger. They are more exposed to the risk of detection for a variety of reasons, but typically the deceased victim's name is 'out of era' with the date of birth on the application form.

Developed identities

This is where the fraudster does not copy another's identity, but instead uses a pseudonym to create the illusion of a real person's existence. They may do this through fraudulent enrolment upon the electoral register, the setting up of utility accounts to obtain bills as 'proofs', and from this collection of paper evidence start opening financial services facilities. These in turn provide the fraudster with more 'proofs', and soon they have an abundance of physical material to pass themselves off confidently in the false name.

Paper evidence of identity – no proof at all

With all of these methods, if the fraudster needs a particular type of proof and cannot obtain an original version, then they may use a forgery. Modern scanning equipment and software packages permit the home user to alter documents and produce forgeries. The more organised professional fraudsters use the Post Office redirection facility to put some distance between themselves and the locus of their crime.

Each method discussed here has its strengths and weaknesses: some methods are easier for lending institutions to detect than others. There are of course many other forms of application fraud, but these are more concerned with the manipulation of status than identity, and for that reason are not covered here.

So who are the fraudsters? What do they look like in terms of profile? And where does it all go on? Profiling reveals that the fraudsters tend to be linked to low-status urban areas, though this is by no means always the case. With previous address impersonation, the profile of the address where the fraudster is currently living is often markedly different from the quoted previous address where the victim is still living. This is obvious — why would a fraudster copy the identity of a person who was unlikely to be creditworthy? Samples show that most fraudsters use addresses that are profiled in the 'high-rise council', 'low-rise council' and 'low-status Victorian' Mosaic bands. Although the age range is substantial, broadly speaking they tend to be male, single, unemployed, and tenants rather than owners. Their crimes are relatively short-lived, with most offences revealing themselves inside a few months, though this can be as long as a year — depending on the sophistication of the fraudster, and their desire to 'sleep' the identity to create the illusion of being a good customer, attract and utilise offers marketed to them through vertical selling, and then abuse all accounts in a short period of time.

Fraudster profile: male, single, unemployed, urban tenant

Examples of cases of transaction and application identity fraud, and the uses of false identities generally, that have been published include the following.

Reported cases in the media

— Five people arrested in Moscow on charges of stealing credit card numbers from Internet retailers and pocketing more than 18m roubles (about £500,000). Police said that the gang stole the numbers of more than 5,400 cards by hacking into websites.[4]

— Nicholas Van Hoogstraten, the most notorious landlord in Britain, has confessed to hiding his £200m property empire behind at least a dozen aliases. The man known as the 'sad Citizen Kane of Sussex' uses false identities to operate as a company director.[5]
— Thousands of credit card users have had their numbers stolen and used to pay for Internet pornography. NatWest and Barclays are investigating after customers complained that mysterious payments for hard-core films had appeared on their statements. Investigators believe fraudsters use a complicated computer scam to access credit card details and then buy porn from American channel RJB Telecom.[6]
— *The Observer* described the alleged activities of Fiona Mont, '. . . the 30-year-old daughter of a prominent Sussex Tory family who has been on the run since faking her own death in January. She has legally held passports in a number of different names to disguise her identity. After changing her name by deed poll, she sends off her old passport and applies for one in her new name. As anyone is entitled to change their name as often as they want, no checks are made at the Passport Office to see whether such changes could be used for criminal purposes. She uses a number of aliases, including Frances Montgomery, Alison Miller, Jacqueline Mayhew and Jamina Chadwick.'[7]
— A man who faced fraud charges faked suicide and fled to the USA. Carl Hilderbrandt obtained a passport using a copy of a dead child's birth certificate in the method used in Frederick Forsyth's *The Day of the Jackal*. His cover was blown in Florida after he was recognised by a tourist from near his home in South Yorkshire. The story was told at Sheffield Crown Court, where Hilderbrandt, 42, admitted theft, obtaining passports by deception and failing to surrender to custody. The original fraud charges had previously been discontinued. He was jailed for 15 months, but will be freed soon because he has been in custody for eight months.[8]
— The *Bristol Evening Post* reported that 'A callous conman is adding to grieving pensioner Christine Cook's misery — by posing as her dead son, Paul. The trickster has taken on the identity of Mr Cook to throw police off his trail whenever he is stopped for motoring offences. As a result, Mrs Cook has received repeated letters and visits from the police. The impostor first struck shortly after Mr Cook died 15 years ago.'[9]

Business identity fraud

Spoofing is damaging to the real business

Returning to e-commerce fraud, there are occasions, albeit few in number, where consumers are duped into believing they are interacting with genuine businesses, which turn out to be fictitious close copies of real business identities. This is known as 'spoofing', where the fraudster(s) load fake websites on to the Internet that look very similar to the genuine company's site, with the aim of collecting information about an individual and their payment card with which subsequently to commit transaction fraud. The victims are numerous and include the individuals who have unwittingly given their identity away to the fraudsters, the genuine company, which has lost new customers and through press exposure may

lose many more potential customers through a lack of trust and loss of reputation, and the card issuer, which experiences lower customer spending and consequent fee income through the real customers' lack of confidence in their plastic.

Scale of the problem

The actual and potential losses arising from application fraud vary according to the measure of fraud prevention diligence applied at the point of account opening. Nearly all banks and other lending institutions have installed sophisticated fraud prevention systems to detect fraudulent applicants with relative ease, and most are members of data-sharing groups in order to prevent repeat attacks. Inevitably there are occasions when the fraudsters surpass these controls, but many organisations prevent more than 90 per cent of their fraud, with less than 10 per cent substantiated. This is a good crime prevention rate, and one which the industry generally should be commended for achieving. The level of identity-related application fraud is tiny, with averaged company figures for 2000 in the region of 0.03 per cent of volumes being reported. Generic fraud is much more prevalent, but still a relatively small percentage of new business volumes.

Most financial institutions have effective counter-measures

APACS, the Association for Payment Clearing Services, reported a huge increase in transaction fraud for 1999, rising to £189.4m from £135m in 1998. In the year to May 2000, total card fraud losses rose by 53 per cent to £226m. 'Card-not-present' fraud (which covers remote transactions and as such is not exclusive to e-commerce) rose 146 per cent to £40m. Sources in the industry estimate that the year to May 2001 could see total figures of around £300m being reported, and indeed the interim figures corroborate this expected escalation.

Spectacular growth in card not present fraud

E-tailers, as opposed to banks, report varying levels of fraud, some of which as a percentage of volumes are high. This is magnified when considering that the tendency is for fraudulent orders to be roughly double the average 'good' order value. The recent Experian survey[10] of 800 dot.coms (conducted in August 2000) revealed that 20 per cent companies were experiencing chargebacks in excess of 1 per cent of sales as a result of fraud; 48 per cent report chargebacks of 0–0.5 per cent; and 8 per cent report levels of 0.5–1.0 per cent. It should also be said that there are anecdotal reports of much higher levels in certain e-commerce markets (see above press reports on transaction fraud), coupled with the fact that 23 per cent of the dot.coms surveyed refused to state what level of chargebacks they were experiencing. Clearly this is a sensitive issue that goes to the credibility of both the specific company surveyed and the channel generally. Interestingly, much higher rates of fraud were experienced where the card origin was overseas, with 23 per cent of the sample experiencing fraud rates of greater than 10 per cent for such customers.

Cross-border fraud a real threat

Solutions

Although it is universally accepted that fraud will never be totally expunged, business has to weigh up the cost of preventing fraud against

the losses incurred through suffering it. There are numerous methods and systems for preventing transaction and application fraud; some are more effective than others, but then they may cost more to implement and maintain.

Domain approach to fraud prevention

Taking transaction fraud first, there are three sites of fraud prevention. One is in the retailer/e-tailer domain, the next is the intermediary payment service provider or merchant acquirer's domain, and the last rests in the card issuer's domain. The retailer is at the front end of the problem, and is best placed to identify the new customer. They can control what questions they ask, and this goes to establishing the validity of the identity. Next they can concern themselves with the verification that the new customer is the 'data subject' of the valid references. Thereafter they can have confidence in the identity of the new customer, and to a certain extent the quality of the transactions that follow.

Reciprocity is crucial to fraud prevention

To obtain 'valid' data and process them to establish 'verification', retailers require the customer's consent and a commercial arrangement with a data verification/credit-checking company to provide the solution. Principles of reciprocity have to be agreed, so their customer data can be used for identification and fraud prevention purposes by other companies contributing data for that purpose. This sort of solution has many advantages, not least data coverage and honed results through scored interpretation of the available data. It also enables other products to be integrated, such as customer profiling, so that once you know who the customer is, their propensities can be more accurately predicted.

The Experian dot.com survey[11] revealed that public data were being used to distinguish between good customers and fraudsters, though only 52 per cent of the sample took advantage of the availability of such data. Table 4 reveals the popularity of the various sources available.

Absence of verification leaves the door open to fraudsters

Of course fraudsters will be able to circumvent these sorts of piecemeal checks. Stronger fraud prevention solutions which call upon a range of public and closed-user-group data are more predictive of potential fraud, but at least the retailers/e-tailers are recognising the need to be diligent in this area, which is appreciated by those organisations further along the transaction chain. Certain payment service providers offer solutions to retailers and e-tailers alike. These solutions identify some fraud from patterns of transactions which taken together appear to be suspicious. This has a certain value, but experience reveals that the introduction of external non-transaction data into the process is more predictive still.

Table 4: Data used to confirm identities

Source	%
Postal address file	61
Electoral roll	39
Telephone file on CD or from bureau	32
Card hotlist from banks	12
BT.com/192.com online directory	19
Internal database	3
Third party to check	3
Other	3

Within the card issuer's domain, systematic fraud prevention is commonplace, with solutions such as Falcon identifying suspicious transactions. Systems such as these use neural networks to learn about the regular or normal pattern of cardholder transactions, and refer out irregular transactions that do not match the cardholder's regular spending behaviour. In addition, the introduction of AVS is expected to identify some, but not all, remote transaction fraud. Ironically, one of the likely effects of AVS is higher application fraud, where the issuer would stand the loss as opposed to the merchant.

AVS initiative likely to cause increase in application fraud levels

Turning to application fraud prevention solutions, these tend to be a mix of data sharing with outcome status, processing with non-status data sharing, and manual systems. Data sharing is commonplace here, with systems such as CIFAS, Hunter and Detect dominating the market. The CIFAS data-sharing system has been in operation for more than a decade, and involves members sharing high-level data about known fraud cases in a database common to all the participating agencies — Experian, Equifax and MCL Software. This system prevents repeat attacks from the same source, and most large lenders, together with a growing mix of other industry sectors, have joined as members. The other 'with-status' data-sharing system is National Hunter (provided by MCL Software), which involves both high- and low-level matching of application data in a time-delayed batch-processing environment. The 'local' Hunter system offers users definable rule setting to recognise application inconsistencies and status matches within the user's own application data universe. The Detect system supplied by Experian offers online real-time fraud prevention, and not only provides matching and inconsistency checking against the shared application database, but also leverages advantages from being housed in a credit reference bureau by accessing shared credit accounts, credit searches and public data — electoral roll, bankruptcies, judgments etc. The outcome of the processing is reflected in the form of a 'fraud index' or score that has been shown to be more predictive than rules-based systems. Both the Hunter and the Detect systems are integrated with the provision of CIFAS data, so in a sense all the systems are cross-supporting.

Experian Detect system leverages ponder of broad data sources

Ensuring online customers are who they say they are and providing a secure and fraud-resistant environment is critical for the Internet seller. New systems and processing are evolving to confirm identity and tackle identity fraud. The Experian e-series identity solution does just this, and relies on Detect-type processing to generate an identity index reflecting the level of confidence in the new customer's identity. Other methods exist, including challenge and response questioning, and the presumption of proof of identity through performance.

Turning to manual methods of preventing fraud, telephone checks to the applicant's home or employer are common, as is the requirement to produce documentary evidence of identity, coupled with anti-forgery checks. The public sector tends to rely on referees to validate the applicant's identity, which is another manual process.

Solutions for businesses to protect customer data from hacking are available, but the newness of the technology and the lack of experience of

developers in deploying enterprise systems are revealed in the exposure of hacked websites. These errors typically come about through not holding sensitive customer information securely enough, or running services other than the Web on the Web server.

Privacy

Privacy and fraud prevention: Balancing rights and responsibilities

The danger with any fraud prevention system is that the objective in preventing fraud is overplayed against the rights of the customer to privacy. The growth in the volume of remote transactions means that more and more personal data will necessarily be stored in the commercial arena, and safeguards need to be set in place to ensure the rights of the data subject are upheld.

The dangers are all too apparent. Robert Scheer, a columnist for the *Los Angeles Times*, and a director of the privacy project at the University of Southern California's Annenberg School, wrote in Yahoo's *Internet Life*, 'Anyone willing to spend a few bucks and a little time on the Internet can find out more about what you read, think and earn than Joseph Stalin or Adolf Hitler could ever have learned about the inhabitants of their totalitarian states.'[12] He suggests that online your privacy rights do not exist. Scott McNealy of Sun Microsystems is reported in the same article as saying 'You already have zero privacy — get over it', as if this is a price worth paying for the wonders of targeted marketing.

In the UK, the Data Protection Act 1998 provides a new legislative base against which the legitimacy of holding and processing data can be established. It is standard practice for larger industry players to interact directly with the Office of the Data Protection Commissioner, or indirectly through their trade association, to ensure their interpretation of the law is *ad idem* with the Commissioner's. That way at least the processing is legitimised, and the rights of the data subject protected. Of course, the Web is a global phenomenon, and so our rights in the UK end on our beaches and are unlikely to be reflected in the same way in other jurisdictions.

Conclusion

We are evolving into a society that will become progressively more dependent on remote interaction with commerce and government alike. The opportunity for fraud will be heightened through ongoing change, which will be advantageous to the fraudster, and impact negatively upon businesses that choose not to be diligent in preventing fraudulent attacks. The tools to reduce substantiated fraud down to a small and manageable level are available, and the proportionate and legitimate use of these may alter the fraudsters' view that for the present time the Internet is their channel of choice.

Internet remains fraudster's channel of choice

References

1. Unpublished survey conducted by Experian in 2000; data drawn from 'Internet Purchasing' section, Nottingham.
2. *Solomon v Solomon & Co.* 1897 AC22 [HL].

3. Experian (2000) *Internet Fraud — A Growing Threat To Online Retailers*, Nottingham, Experian.
4. *The Guardian* (2000) 29 April.
5. *Independent on Sunday* (2000) 3 September.
6. *Sunday Express* (2000) 2 July.
7. *Observer* (2000) 20 August.
8. *The Times* (2000) 21 April.
9. *Bristol Evening Post* (2000) 18 August.
10. Experian, ref. 3 above.
11. *Ibid.*
12. Scheer, R. (2000) 'Nowhere to hide', *Internet Life*, October.