Internet fraud:
A growing threat to online retailers

Contents

1

Executive summary and key findings from the research

During August 2000, Experian commissioned an independent research agency to conduct one of the most extensive analyses to date on the effect of Internet fraud on UK retailers. The agency approached 800 online retailers to establish the extent of Internet fraud, its operational impact, the effectiveness of current fraud prevention systems and, finally, to identify common features in the way Internet fraudsters operate.

The survey revealed that Internet retailers are proving easy prey to credit card fraudsters, made easier by the absence of online fraud detection systems and a police force unable to tackle this new type of crime. In consequence, online retailers are increasingly becoming victims of repeated, opportunistic and unsophisticated fraud.

The survey showed that online retailers either do no checking or rely almost totally on manual fraud prevention measures. Almost half said they did not use any external data when verifying a customer's name and address, before authorising an online transaction.

The headline findings from Experian's research were as follows:

- Nine in every ten Internet fraudsters are getting away with it! The survey revealed that the police are unable to deal with this new type of retail crime with 57% of companies saying that they had reported frauds to the police but 53% encountered a lack of interest. Only 9% of frauds reported by online retailers to the police resulted in prosecution.
- 70% of companies interviewed thought that the internet was inherently more risky than other routes to market, with the majority of respondents experiencing an increase in fraud on the Internet over the last year. 52% of online traders claimed that Internet fraud was a problem for their organisation and 55% said it was a growing problem.
- Retailers become aware far too late when they have been victims of fraud. Almost half the companies interviewed (48%) said it could take more than a month before they are made aware they were victims of card fraud. 18% said it took up to seven weeks.
- 40% of companies said that they had been hit by the same fraudster more than once, with 18% saying that they had been hit three times by the same fraudster before the fraud was detected and the account closed.
- 11% of respondents admitted that their site had been hacked into.
- Only 15% of companies said they had automated systems for detecting fraud. The vast majority still employ expensive and inaccurate manual processes. Only 52% use any external data to verify a customer's name and address.
- Fraudsters have realised that methods of prevention are currently so inadequate they need spend little time or effort covering their tracks. Less than 10% of fraudsters bother with a redirection service at the goods delivery address, and only 10% make the effort to set up a false telephone account.
- In order of incidence, the most common features of the card fraudster's modus operandi are as follows: "Using a real name at a real address but not the cardholders name" - this shows that fraudsters will typically copy identities of previous residents associated from the

premises from which they are operating. Next most common was using "cardholder's name at a real address but not the cardholder's address". It suggests that the fraudsters often have information about the real name of the cardholder. Third most common with "false name at real address" exposes the interception or illicit generation of credit card numbers. Finally, "cardholder's genuine name and address, but parcel delivered to another address" shows that certain fraudsters will hijack not only the card number, but also the cardholder's real identity and address creating the illusion of a completely genuine transaction.

- 58% of companies thought that the fear of fraud was a significant barrier to successful trading on the Internet.
- Although Experian's own client experience suggests an average level of chargebacks of some 2.5% sales, the survey indicated that retailers are experiencing lower than expected levels of fraud chargebacks. It suggested that 20% companies are experiencing chargebacks in excess of 1% of sales as a result of fraud. 48% report chargebacks of between 0-0.5%, and 8% report levels between 0.5-1.0%. This might suggest that online retailers are reluctant to reveal the true extent of their online fraud problem.

2

Methodology and approach; description of retailers involved, sector analysis, size of the companies, numbers of employees, average value of online transactions and the split between telephone and internet sales.

Some 800 online retailers were approached in the telephone-based survey. Experian commissioned an independent BRMB accredited agency to conduct the research over a two week period in August. The questionnaire comprised 40 detailed questions, primarily concentrating on the issue of fraud but also asking a range of general questions about the experience of online trading and other issues associated with the Internet. The size of the companies that responded, defined in terms of employee numbers, were largely on the smaller side (66% with up to 49 employees), which is typical of most online retailers. The responding sample can be described as follows:

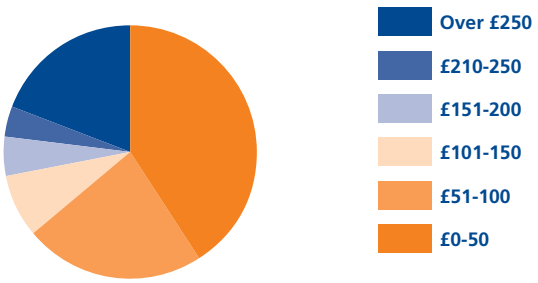
0-49 employees	66%
50-199 employees	15%
200-499 employees	5%
500+ employees	5%
1000+ employees	9%
5000+ employees	4%

The sample represented an even balance of dot.coms (52%) and clicks and mortar companies (48%). In terms of sectors represented in the analysis, we have further defined the sample in terms of the following retail product categories:

Music, CDs, DVDs	6%
Audiovisual, telecoms	8%
Books	4%
Multi retailers	22%
Software, games	13%
Sports equipment	5%
Jewellery	2%
Wines, hampers, chocolates	8%
Travel, Tickets	8%
PCs, hardware, printers	5%
Clothes, fashion	9%
Beauty products	1%
Auction	1%
Furniture, flooring	5%
Tools, garden equipment	3%

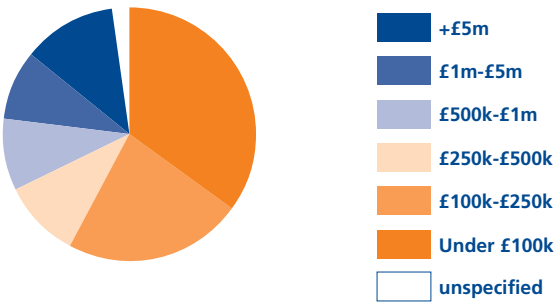
Looking at the size of online orders, 41% of the sample said the average value of their online orders ranged between £0-£50; 23% said it was £51-£100; and 19% said it was over £250 (see table).

Average size of online orders



Looking at actual values, it is estimated that the survey represents around £600 million per annum of online trading. A significant proportion of the sample (35%) said they had online business worth up to £100,000 per annum; however 23% said it was between £100-250k; and 21% of the sample transacted over £1 million per annum online, 12% admitting to more than £5 million per annum (see table).

Average value of online orders



Regarding the split between telephone and Internet sales, 77% of the sample said that they took orders over the phone as well as the Internet, 13% just took orders over the Internet and 10% just took orders over the phone.

On a general note, the overwhelming majority (96%) said they conducted business online with Card Not Present (CNP) transactions and 95% said their goods were of interest to thieves.

On the perception of fraud, 52% claimed that internet fraud was a problem for their organisation. Added to this, 58% companies thought that the fear of fraud was a significant barrier to successful trading on the Internet and a similar number (57%) said that they had experienced an increase in fraud since using the internet as a route to market. Finally, 52% experienced a higher rate of fraud on the internet as opposed to other routes to market and the vast majority (70%) thought that the internet was inherently more risky than other routes to market.

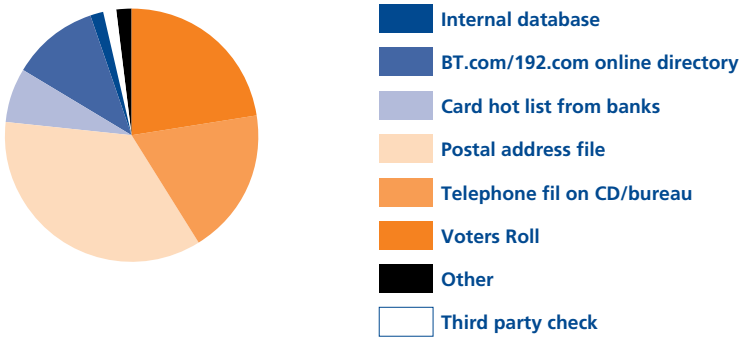
3

An assessment of existing fraud detection systems, whether manual or automated, the cost of fraud detection per transaction, the use of external data to verify identity and point of sale checks.

The report revealed a low take up of automated fraud detection systems in place, suggesting that products are scarce or not being used if available. This suggests that current automated solutions are too expensive. 55% employed manual fraud detection systems with only 15% of the sample having automated systems.

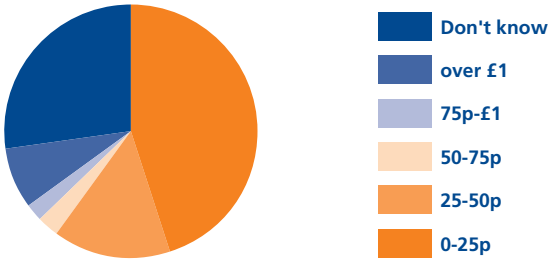
Just over half (52%) said that they used external data to verify either the name and address. Of this number that used external information sources, 61% said they used the Postal Address File, which only verifies that an address is genuine and does not link address to name. Only 39% used the voters roll to verify name and address links; 29% used a telephone CD or bureau service to verify phone numbers and just 12% checked with a Card Hot list (APACS) to see whether the card number belonged to a stolen credit card.

External datasets used by 52% of the sample were given as follows:



The survey also revealed that the cost of fraud detection per transaction was surprisingly low, with 45% of the sample estimating the cost of fraud detection per transaction between 0-25p per transaction; 15% said it was between 26-50p; 8% said it was worth more than £1.00 per transaction, and 27% did not know what the cost was (see table).

Estimating the cost of fraud protection



Only 25% of the sample asked for a work email alongside home email for added verification when taking an order.

When asked what fraud solutions were most needed, a majority (63%) identified an urgent requirement for instant online personal identity verification systems that checked both name and address and linked card holder details with billing address. Many mentioned that more was required from the banks and card issuers to ensure this was met.

4

Levels and types of fraud suffered by online retailers. Analysis of chargeback levels and the most common characteristics of online fraudsters (the typical modus operandi).

Chargebacks occur in CNP transactions when a fraud has been committed. A CNP transaction i.e. when goods are paid for without the card being present, is the primary means of transacting online. The cost of fraud in a CNP transaction is nearly always met by the online retailer, not the genuine customer whose card details have been compromised. It should also be pointed out that not all chargebacks are frauds - sometimes the customer denies a transaction that they actually conducted. Also some will refer to instances where goods were ordered but not delivered.

The online retailer bears all the risk in a CNP transaction because, unlike a retailer in the "real world", they do not take an imprint of the card. Normally a fraudulent transaction is spotted when the genuine card holder notices a transaction on their credit card statement which is "not theirs". They report this to their card issuer and, inevitably, the full value of the transaction is "charged back" to the retailer while at the same time a credit is made to the genuine customer's account. Despite a common misconception, the consumer rarely loses out in cases of online card fraud; all the risk is borne by the online retailer.

Card issuers (Merchant Acquirers and Payment Service Providers) have different policies regarding the level of acceptable chargebacks. If chargebacks exceed agreed percentage levels over a pre-determined period then issuers will, and do, impose penalty fees. In some cases this may involve revoking or suspending the merchant's licence, which would prove fatal to single-channel online traders. It is therefore vital that Internet retailers do all they can to keep chargebacks to a minimum and this may mean implementing more effective fraud preventative measures.

For the reasons explained above, the issue of chargebacks is highly sensitive to online retailers, and it is difficult to assess the true extent of the problem. In some cases, online retailers will actually meet the cost of fraud personally, to avoid higher chargebacks and the risk of losing their merchant's licence. This said, 48% of the sample admitted to 0.5% chargeback as a result of Internet fraud; 8% said their level was up to 1% and 20% said that their levels were in excess of 1% of total transactions. However, a significant proportion (23%) refused to give an answer to this particular question.

Up to 0.50%	48%
1.00%	8%
1.50%	3%
2.00%	3%
3.00%	3%
4.00%	2%
4.50%	2%
5.00%	2%
5-10%	2%
10%+	3%
Refused to say	23%

When estimating true levels of chargebacks, one needs also to remember that a number of genuine transactions are denied by the card holder for whatever reason. In this respect, 47% of the sample reckoned that up to 5% of transactions denied by the cardholder were actually genuine.

Experian's research sought to understand the typical modus operandi of fraudsters as a means of predicting behavioural patterns and identifying likely fraud scenarios for the development of more effective fraud detection systems.

It identified one of most common features of CNP fraud as "real name at real address but not the cardholders name". In other words, the fraudster had given a real name and address (which would be verified by the voters roll), probably a name and address supplied to the VR for the purpose of fraud; but the card number given matched a different name. This suggests inadequate procedures for linking name, address and card holders name.

The next most common modus operandi "Cardholders name at real address but not cardholders address" suggests that fraudsters are giving names to match the account name but the address provided does not match the billing address, suggesting again that there needs to be a link between billing address and delivery address.

False name at real address was also a common tactic, but this could only work where no reference to voters roll was made when authorising the transaction. This lack of checking is borne out by other findings in the research and could be prevented by a simple automated check of the voters roll.

Finally, "Cardholders genuine name and address but parcel delivered to another address" illustrates a dilemma faced by online retailers that despatch goods to addresses other than the card holders 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.

A significant finding was the evident lack of sophistication in the modus operandi of Internet fraudsters. It appears that systems for verification are so inadequate that fraudsters need spend little effort covering their tracks. In the experience of most online retailers, around 10% of fraud takes place with a re-direction service at the end of it and only 10% of frauds occur with the fraudster having opened a telephone account in a false name.

Another issue relates to the time delay in identifying that a fraud had been committed. In this respect, the majority of fraud becomes apparent after six weeks. 33% of companies said it took over two months (8 weeks+) before being notified that they were victims of a fraud and 18% said it took between 4-7 weeks. During this time, their site was vulnerable to repeat attacks. Interestingly, although the majority said fraudsters tended to hit once on average, a sizeable number said they were hit twice and 18% said they were hit three times on average by the same fraudster before the fraud was detected.

In fairness, the time delay is often due to the fact that the genuine cardholder has yet to open their monthly statement and report "unknown transactions" to the issuer. This process initiates the chargeback scenario mentioned in section three of the report. But there are cases when the genuine cardholder, for whatever reason, fails to open and check their statement.

5

Overseas trading. Which countries are most traded with, the constraints identified with transacting with overseas customers, billing and delivery factors, the level of fraud originating from overseas transactions.

Online retailers were questioned about the problems they faced when attempting to authenticate overseas customers. Of those that traded overseas, the most common response was that there was a lack of data available to verify whether a name and address provided by a customer was genuine (33% of all companies).

When asked what problems companies faced when trying to establish whether a customer was genuine, the response can be summarised as follows:

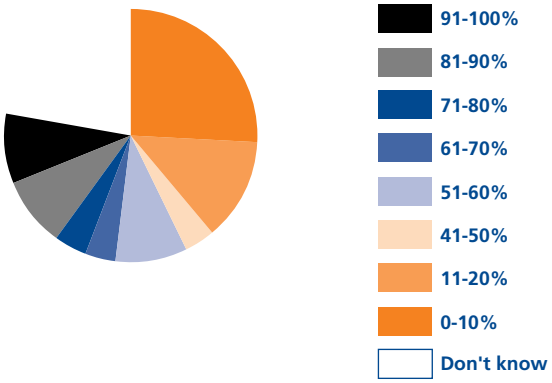
Have problems identifying the card issuer.	22%
Don't accept non UK customers or conduct business overseas	45%
No way of finding whether an overseas customer is genuine through absence of effective databases.	33%

In this respect, the survey identified a clear reluctance to trade with non-UK customers. 60% of the sample said that only 10% of their Internet business was conducted with overseas customers; 12% said it was between 11-20%. (see table):

0-10%	60%
11-20%	12%
21-30%	8%
31-40%	2%
41-50%	5%
51-60%	2%
61-70%	2%
71-80%	2%
Don't know	3%
None	5%

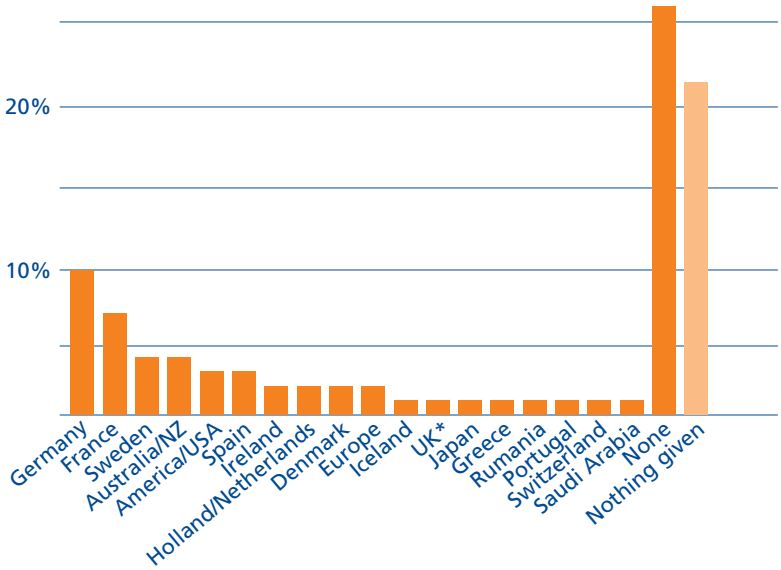
Looking at fraud levels, there was a clear indication that overseas business was more prone to fraud. 26% of the sample said that up to 10% of non-UK card transactions were fraudulent; 13% thought it was between 11 and 20%; 22% didn't know the answer (see table below).

Percentage of non-UK transactions which were fraudulent



Although a proportion of the sample were US companies it is still surprising to see how UK dominated e-commerce sales are - given the universal nature of the Web. With credit cards being the dominant payment method on the Web it is unlikely that this is what is holding merchants or customers back.

When asked which countries they did most business with overseas the rankings were as follows:



*UK is overseas for those US companies surveyed.

The dominant business partners - Germany, France and Sweden are also close geographically to the UK and near the top of the list of 'wired' European countries when expressed as a percentage of the population with online access.

When asked how important overseas customers were to their business over 67% said it was very or somewhat important. However, 64% put only 0-10% of their current customer base as residing outside of the UK.

6

Logistics. Cost of logistics as a per cent of online sales, requirement for card imprints at point of delivery, shipment to addresses other than billing address.

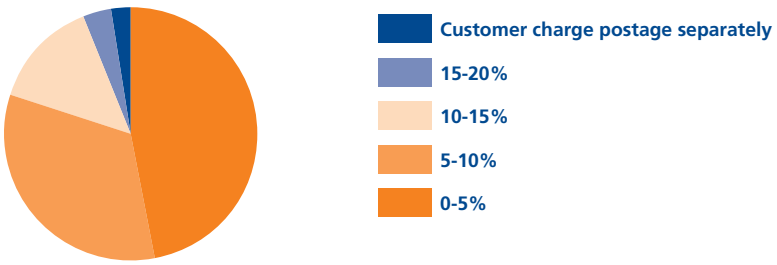
96% of the businesses surveyed accept CNP transactions with most transactions around £100.

Delivery of the goods is then just a matter of moving them to the address specified. One important way of preventing fraud could be provided by the delivery mechanism. 60% showed an interest in card imprints being taken at the point of delivery, with 80% interested in this solution for goods up to £100.

Significantly just under half of those surveyed (45%) would only deliver to the billing address. However, many felt that delivering to other shipping addresses was not particularly prone to fraud.

The impact of the logistics of delivery on costs of sales was significant with around 30% of businesses saying that it formed between 5-10% of the total cost of sales for the business.

Logistics cost as proportion of sales



7

Visitor website analysis. Types of methods currently available, use of segmentation systems to predict likelihood of fraud, personalisation, clickflow analysis, most common methods of website customer analysis indicating the current lack of effective analyses.

The development of web traffic analysis and personalisation tools has been driven mainly by the need to segment potential visiting customers more effectively and so improve profitability. Until recently the most common form of profiling is to take the log files that web servers generate automatically and, using analytical software to generate a traffic analysis. Although providing basic information on visitors - such as overall numbers and the most popular pages - the information is entirely anonymous and it is impossible to track visitors from one session to another - unless they register in some way or are given a cookie.

Unless you register your visitors there is no way of tracking them from visit to visit. One approach is to add a small piece of code called a cookie to the visitor's hard drive. Next time they come to your site your web server searches for the cookie. If it finds one then it can serve up some personalised content. Many people don't like cookies, however, and turn them off at their web browser. There are various privacy issues to be considered - and the types of information that can be stored in a cookie are severely limited.

A more advanced form of visitor profiling is called psychographics. This involves examining the clickstream of visitors and comparing it to the records of previous visitors. For example, a customer clicking on an advert for a new Stephen King novel will be compared to the profiles of other customers also interested in Stephen King. If they also bought Frederick Forsythe novels then the new customer will also be offered Frederick Forsythe. This is how Amazon.com analyses visitor traffic. Psychographics is a useful commercial tool but it still tells you very little about the individuals accessing your site. It can also be prohibitively expensive being used mainly by only the largest e-commerce organisations.

The latest form of visitor profiling - available in Experian's e-series range of products and services - provides access to a range of information sources from geodemographic databases to credit histories. This kind of information not only allows businesses to profile customers but to do everything from pre-screening for offer suitability, to online credit applications and, of course, prevent fraud.

Our survey revealed a marked lack of serious visitor profiling activity. More surprisingly a third of those surveyed did not even measure the size of their web site communities - an ability provided by even the most basic of web analysis tools. The more established marketing tools from the offline world have moved online with over 50% of those surveyed analysing their visitors in terms of ABC1s and so on. However, on the whole, this kind of analysis only applies to existing customers who have registered in some way.

41% do measure customer lifetime value and 67% measure visitor to sales conversion rates - although these are likely to be a natural consequence of existing accounting systems - coupled with an analysis of standard log files. In such a highly pressured and competitive environment it is surprising that only 26% use any external data to analyse visitors to their sites - and those used were mainly for purposes of fraud prevention and not to improve the customer experience. There is perhaps some correlation with the finding that shows only 18% said that they personalise web sessions in any way. Over 60% of web sites do not have an inbuilt real-time decisioning processes.

8

Legislation and due process. Effectiveness of current legal process in prosecuting Internet fraudsters, police constraints and limitations, attitude of online retailers as regards pursuing fraudsters, preferred means of civil recovery.

The survey seems to back up the commonly held belief that the prosecuting authorities do not have the resources to counter fraud online.

Merchant sales revenues are not assured when accepting CNP transactions. This is because the merchant cannot examine the card, nor obtain a signature for comparison. Consequently, authorisations are limited to checking the account has available funds, and is not reported stolen. Excessive charge back rates can threaten the merchant's relationship with their Merchant Acquirer.

Nine out of ten fraudsters are getting away without prosecution - with 40% going back to the same Web site more than once to commit the same crime.

The United Kingdom has devoted little dedicated resource to what has become the fashionable new and almost risk-free crime. In the US there is a department of over 200 people whose sole job is to look for suspicious e-commerce sites which may be used for 'harvesting' credit card numbers. In the UK the equivalent department consists of just 6 people.

In the rush to get online, businesses seem willing to compromise security when building their e-commerce operations. Many are also unaware of just how little help the law and the enforcing authorities appear able to give.

Less than half (43%) of those surveyed reported any frauds to the police and over half of those (57%) who did encountered 'lack of interest' from the police.

More worrying, in only 9% of cases reported to the police was a prosecution set in motion.

In 12% of cases the business attempted to recover the money defrauded themselves - most of them opting for a debt recovery agent.

Fraud recovery

- If delivery was to a genuine address obtain an order to search those premises
- If the property is in the fraudster's name, obtain an order 'freezing' the property
- Find out anything else about the fraudster, particularly about his or her possessions, and freeze those as well
- If all else fails, take advice as to what claims you may have against a web site designer who may not have ensured a secure web site.

9

Internet usage - a survey of 500,000 consumers. The number of people purchasing on the Internet has more than doubled between January and December 2000, according to the latest research by Experian, the global information solutions company. 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 and with the most popular items being holidays, books, computer games and music.

The findings have been gathered from a survey of over half a million Internet users as part of Experian's Canvasse Lifestyle survey questionnaire. 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 twelve months, as well as a breakdown of the age, income, purchasing frequency and types of products purchased by online shoppers.

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 twelve months has more than doubled from 5.1% (2.26 million adults) at the beginning of 2000, to 10.7% (4.7 million adults) in December 2000.
- Some 3.3% of the UK adult population - around 1.45 million people - have made four or more purchases since the start of 2000. At the same time, the proportion of adults that bought just once in the 12 months to December 2000 has decreased from 35% to 27%, but the proportion purchasing four or more times over the same period has increased by over a quarter from 24% to 31%. This suggests that people are starting to purchase more frequently.
- 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% to 17% 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.
- Internet shoppers are mainly younger and wealthier people. Measured against the national norm, the age group most over-represented amongst online shoppers is 18-25 (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 over-represented at almost 166% of national norm, whereas 36-45 year olds are a fifth up on the national average. The survey 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%), while just 22% said that it was valuable. The remainder (41%) were neutral on this question.

Results of Canvasse Lifestyle Internet Survey

% online purchasers	% Adults
January 2000	5.1%
December 2000	10.7%
Volume online purchasers	**Actual Counts**
January 2000	2261600
December 2000	4708000
% online purchasers - frequency	**% Adults**
Total	10.7%
Once	3.0%
2-3 times	4.4%
4+ times	3.3%

Internet Shoppers - Income Split	**Internet Shoppers**	**UK Average**
£0-19000 p.a.	33%	65%
£20000-39000	42%	27%
£40000-60000	16%	6%
Over £60000	9%	2%

Internet Shoppers - Age Split	**Internet Shoppers**	**UK Average**
18-25	9%	4%
26-35	27%	17%
36-45	25%	20%
46-55	19%	18%
Over 55	20%	41%

Internet Shopping by Products	**January**	**December**
Holidays	14%	17%
Books	28%	29%
Children's Clothes	2%	2%
Computer Games	12%	12%
Fashion Wear	8%	6%
Financial	4%	1%
Health	3%	1%
Music	18%	21%
Garden	3%	2%
Video	6%	7%
Wine	3%	3%

Changing online purchasing habits - 2000	**January**	**December**
Once	35%	27%
2-3 times	41%	42%
4+ times	24%	31%

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 an average Internet purchase of £50, we estimate that Internet sales have more than doubled over the past year, growing from £264 million at the start of January 2000 to £602 million at the beginning of December 2000.

Talbot House
Talbot Street
Nottingham
NG1 5HF
T: 44 (0)115 934 4473
F: 44 (0) 115 934 4704
www.experian.com