

CyberSource®
the power of payment

Second Annual

UK Online Fraud Report

Online Payment Fraud Trends and Merchants' Response

2006 EDITION

Sponsored by CyberSource





List of Figures

- Chart 1. Main Payment Types Offered in 2005
- Chart 2. Primary Online Fraud Concerns
- Chart 3. Factors Key to Reducing Fraud
- Chart 4. Risk Management Pipeline
- Chart 5. Fraud Management Methods in 2005
- Chart 6. Manually Reviewed Orders Ultimately Accepted
- Chart 7. Manual Review Techniques in 2005
- Chart 8. Online Sales Expectation for 2006
- Chart 9. Fraud Management Tools Planned for Implementation
- Chart 10. Manual Review Staffing Levels for 2006

Table of Contents

Page

| | |
|--|----|
| Executive Summary | 4 |
| Key Findings and Analysis | 5 |
| Conclusions | 6 |
| Benchmarking Fraud Management Practices | 7 |
| Plastic still number one payment preference | 7 |
| Overseas ambitions continue to burgeon | 8 |
| Fraud moves further up merchants' online agendas | 8 |
| Revenue growth outstripping fraud increases | 8 |
| Merchants mindful of evolving fraudster methodologies | 9 |
| Further recognition of anti-fraud technologies | 10 |
| Indirect costs of online fraud still high | 11 |
| Manual review remains strong line of defence | 12 |
| Most manually reviewed orders accepted, but at a price | 13 |
| Managing Online Fraud in 2006 | 15 |
| Merchants' upbeat on growth – massive revenue increases forecast | 15 |
| Implementation of authentication systems planned | 16 |
| Little change expected in order review staffing | 16 |
| Conclusion | 17 |
| Risk Management Solutions | 18 |
| About CyberSource | 18 |

Methodology

This report is based on a survey of merchants drawn from a broad cross section of organisations, for which the UK market represents their main source of online revenue.

The survey was designed to encompass a representative range of small, medium and large companies with UK offices. The majority of respondents have more than five years of experience selling online, although participants ranged from businesses in their first year of online trading to some of the largest and best-known companies in the world. The survey was carried out through a combination of online questionnaire and telephone interviews.

In total, one hundred and sixty merchants took part in the survey, which was conducted over two weeks in September 2005. All respondents were either personally responsible for, or influenced, decisions regarding risk management in their companies.

Comparisons are also made with the online fraud survey conducted simultaneously in the US by CyberSource Corporation.

Summary of Participants' Profiles

| Online Fraud Survey | 2004 | 2005 |
|---|-------------|-------------|
| Total number of merchants participating | 104 | 160 |
| Annual Online Revenue | | |
| Less than £250K | 45% | 17% |
| £250K to less than £5M | 35% | 51% |
| Over £5M | 20% | 32% |
| Duration of Online Selling | | |
| Less than one year | 17% | 9% |
| 1 – 5 years | 50% | 41% |
| 5 or more years | 33% | 50% |
| Risk Management Responsibility | | |
| Ultimately responsible | 50% | 36% |
| Influence decision | 50% | 64% |



executive **summary**

In recent years, with online commerce continuing its apparently irresistible push into global buying habits, the world has also witnessed the growth of another, less welcome phenomenon – online fraud.

In this, the second annual UK Online Fraud Report conducted by CyberSource, we revisit the issues tackled for the first time in 2005's inaugural report – namely the prevalence, detection, prevention and management of online fraud in relation to UK businesses.

This comprehensive study addresses all the pertinent areas, summarising the major findings and including detailed analysis. The document additionally profiles the key issues and trends – which this year have seen a number of pronounced and definite developments.



key findings *and* analysis

Merchants prevailing in the battle against online fraud

It is evident from the results of both last year's survey and this one, that the struggle against online fraud has now been almost universally recognised as an issue central to the future success of web-borne commerce. Companies are continuing to take appropriate steps and would appear to be treating the threat ever more seriously.

Respect for the problem has grown still further through the twelve months between the 2005 and 2006 reports – with the last year proving to be a period during which a number of key shifts have taken place in anti-fraud techniques and attitudes.

Crucially, while Internet fraud has again risen as a total amount during the last year, for a number of merchants it actually fell as a proportion of overall online transactions and spend. Put simply, for these businesses the growth in online trade is significantly outstripping that of online fraud.

This trend would appear to have developed, in the most part, from organisations treating the issue of online fraud as central to their focus and strategy.

It is clear though, that this stance must continue if the online business community is to avoid a relapse as fraudsters further hone their skills to challenge the growing sophistication of anti-fraud solutions.

Chip and PIN worries mellow as other concerns come to the fore

The continuing penetration and acceptance of chip and PIN-governed transactions in the bricks and mortar world again registered as one of the key concerns for online retailers. However, whilst it is still felt that chip and PIN will encourage fraud to migrate online, the threat is deemed to be at a much lower level than that detailed in the 2005 report.

Other factors rose up the list to take its place, with evolving fraud techniques and the growth of identity theft among those causing the most disquiet.

While around a fifth of respondents felt that chip and PIN would continue driving fraudulent activity on to the Internet, many more participants were troubled by a perceived increase in the sophistication of fraudsters (39%) and a higher incidence of identity theft (35%).

Together these three factors constituted the bulk of the concerns; between them being cited by 92% of participants.



Reliance on manual review continues

Of the tools currently being used by companies to manage online payment fraud, manual review remains a firm favourite – in terms of popularity it is second only to Card Verification Number (CVN - a number printed on the front or back of many credit/debit cards; also known as CVV, CVV2, CID, CSC etc.). With evidence that much of this effort may be unnecessary, it is an issue that will require closer attention if organisations are to maximise the efficiencies of their online operations.

Most companies maintaining manual reviewing regimes recognised, for instance, that the majority of suspect orders assessed eventually go on to be processed in full (over two thirds of merchants surveyed accept 80% or more of orders that have been manually reviewed).

By far the most popular form of manual intervention remains direct customer contact (via telephone or email), followed by communication with the customer's bank, checking order histories and negative lists, and consulting third parties – all of which were roughly on a par.

Most merchants expected manual review staffing levels to remain static in 2006, whilst only a quarter predicted a rise.

Massive growth in sales predicted

Respondents expected their online divisions to generate an average of £9.52 million in revenues during 2005.

The overwhelming majority – more than 90% – of the companies surveyed envisaged a substantial uplift in online revenues for the 2006 trading period, with almost three in five predicting growth of 20% or more.

Confidence growing in anti-fraud technologies

There are firm indications that organisations are now recognising the advantages of automated checking and authentication systems – almost seven out of ten respondents to this year's survey counted such tools in their anti-fraud armouries.

Comparatively few merchants have plans to introduce any further measures during the next year and, whilst this suggests an encouraging growth in their faith in existing techniques and systems, organisations must be cautioned to guard against over-confidence.

Conclusions

One of the most crucial of this year's findings is that, while still rising as an overall amount, Internet fraud now looks to be falling as a proportion of online spend. In light of how fast online retail culture and spend is currently growing this represents an important shift.

Elsewhere, increasing numbers of eCommerce businesses have invested in emerging anti-fraud techniques to save themselves time, money and resource. These in turn are enabling merchants to refocus their energies on more strategic and, arguably, more important challenges such as driving for greater efficiency, customer satisfaction and profit.

Further evidence of such a trend is clearly visible in the survey's online growth forecasts for the next year. A substantial upsurge in revenues was predicted by the majority of those surveyed, with only a tiny percentage expecting profits to remain static.

Overall then, this year's results paint an encouraging picture. But not one that yet spells any kind of dissipation of the underlying threat.

While the UK's major online retailers do seem to be winning, or at the very least rallying, in their battle against online fraud, cyber criminals will continue, as they always have, to refine and hone their methods and techniques. Just as one threat looks to have been identified, another will invariably rear its head.

Tackling fraud therefore remains as tough and as tall an order as ever – an evolving challenge that requires ongoing investment and determined long-term commitment.

benchmarking *fraud* management practices

Main Payment Types Offered in 2005

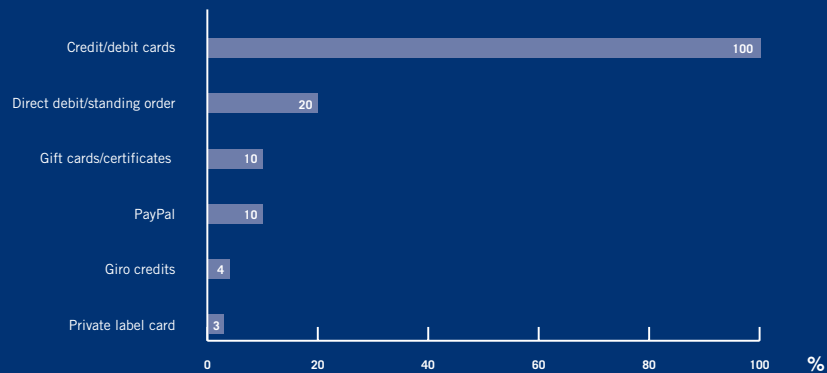


Chart 1

Plastic still number one payment preference

Prior to examining UK online fraud developments it is useful to focus on the payment types most commonly accepted by eCommerce businesses. Credit and debit cards remain easily the most popular form of payment acceptance, with around five times as many merchants accepting credit and debit cards compared with standing order and direct debit payments (Chart 1).

Currently, more than ten times as many respondents accept plastic cards than either PayPal or gift certificates. Merchants should be aware that the growing popularity of these emerging online payment methods may require different fraud management techniques to be utilised in the future.



Overseas ambitions continue to burgeon

Whilst uncertainty about eCommerce remains an issue with regard to consumer confidence, businesses appear more upbeat, with almost four out of five (78%) of the merchants surveyed now accepting orders from outside the UK – proof that many organisations are seeking additional revenue opportunities in a global marketplace.

Whilst international markets represent an attractive opportunity, online merchants must ensure that their fraud detection systems are robust enough to handle the additional risk involved. Furthermore, international fraud risk varies by region with both UK and US survey respondents citing Nigeria as posing the highest risk. It is essential that fraud management practices be customised so that they meet the challenges created by some countries.

Fraud moves further up merchants' online agendas

Following confirmation in last year's report that online fraud is now recognised by web-based businesses as a prime concern – and that it is being treated accordingly – this year's responses indicated that the issue is rising still higher in business consciousness and company focus.

Online fraud is now seen as a priority at least on a par with business continuity, accepting foreign orders and price competition. Only customer satisfaction is rated a higher priority overall, with merchants recognising that customer loyalty is vital for online success. Anti-fraud tools that offer real-time responses provide the consumer with a seamless experience, increasing customer confidence as well as the likelihood of return visits to the website.

Revenue growth outstripping fraud increases

As a total sum, online fraud again rose through 2005 – but not in proportion to transaction volumes and spend. Around a third of respondents (35%) noted no change in their incidences of fraud, and almost a third (30%) said that they had fallen. Therefore, as a total sum fraud was found to have remained static or fallen in almost two thirds of cases (65%).

When considering fraud as a proportion of total revenues, just 16% of participants reported it as rising. More than half (53%) said that online fraud had remained at the same level, while almost a third (31%) noted that it had fallen.



Merchants mindful of evolving fraudster methodologies

While a fifth of respondents predicted that chip and PIN would drive fraud on to the Internet and cited this as a primary concern, more (39%) were concerned about perceived increases in the ingenuity of fraudsters. Nearly as many merchants (35%) noted the growing prevalence of identity theft as a headline issue (Chart 2), demonstrating that this has become a very real concern among online traders.

These three key issues together accounted for the main fraud-related concerns of more than nine out of ten of those surveyed (92%).

Primary Online Fraud Concerns

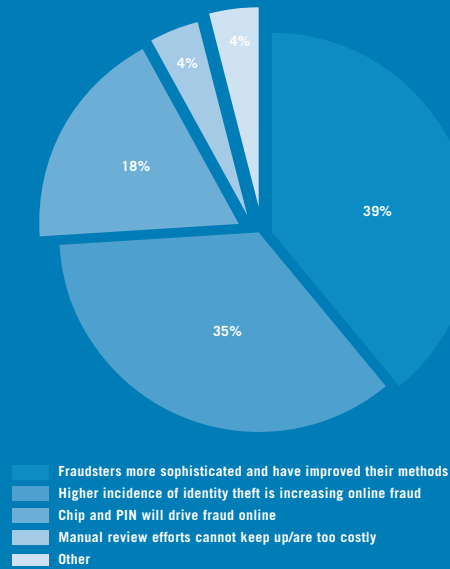


Chart 2



Factors Key to Reducing Fraud

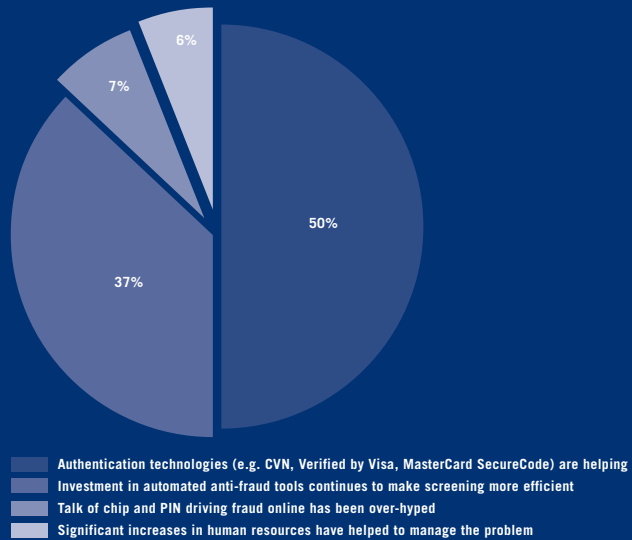


Chart 3

Further recognition of anti-fraud technologies

Respondents believe that the growing sophistication of anti-fraud tools and techniques will play the biggest part in bringing online fraud down still further, with a massive 87% citing such tools and authentication technologies as key (Chart 3).

Other factors, such as human resource levels, were seen as less significant, indicating that companies have an increasingly mature and thorough understanding of the elements needed to effectively combat the problem of fraud.

It also suggests that UK businesses are becoming more cognisant of the threat (and the factors that impact it) than previously, and are therefore less likely to 'bury their heads in the sand' or misplace resources by looking to address non-core issues.

Indirect costs of online fraud still high

In order to fully understand the true impact of online fraud, the survey examined both its direct and indirect costs.

The total cost of fraud =

- the cost of tools/systems to review orders
- + the cost of rejecting orders (some will be valid)
- + the cost of manual order review
- + direct fraud loss and associated administration

An order pipeline is used to demonstrate these costs (Chart 4). Transactions enter the pipeline, are evaluated by detection tools and automated decisioning systems, and may then be subject to manual review. To quantify the total cost merchants should examine each point in the pipeline.

Risk Management Pipeline

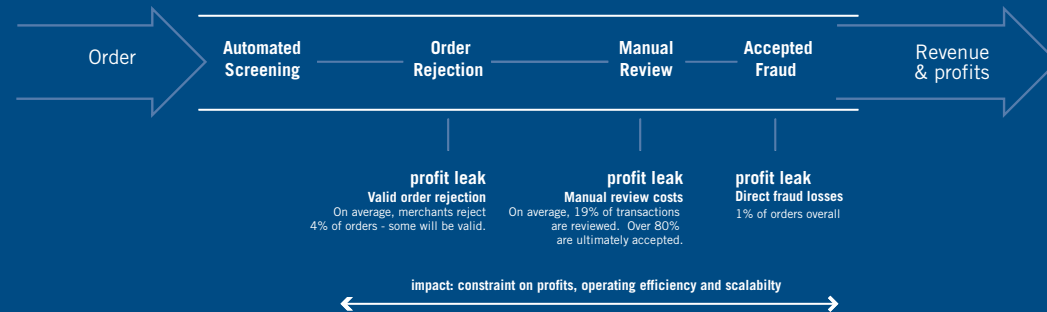


Chart 4

Order rejection The diagram above illustrates that merchants are declining 4% of orders due to suspicion of fraud; a 2% decrease from the 2004 survey. This reduction is mirrored by the results of the US survey, where the overall order rejection rates have fallen from 5.9% to 3.9%.

Manual review Another major indirect cost concerns manual review. Indeed, respondents indicated that they are manually checking 19% of all incoming orders, an area that is covered in more detail later on.

Accepted fraud The UK survey also found that 1% of accepted orders turned out to be fraudulent, down from 1.6% in the 2004 survey. This matches the US finding of 1%, a decrease of 0.3% from last year's result, suggesting that organisations on both sides of the Atlantic are starting to manage their risk processes more effectively.

Chart 4 shows that these profit leaks can impact up to 20% of total incoming orders, posing a serious threat to business growth. Merchants that focus their efforts on improving the level of efficiency across the pipeline stages can achieve a significant increase in profitability and scalability.

Manual review remains strong line of defence

Of the range of methods and tools currently being employed by companies to minimise the impact of online payment fraud, the three most widely used continue to be Card Verification Number (CVN), Address Verification Service (AVS) and manual review (Chart 5). CVN is now the most popular tool, up from number three in the 2004 survey.

The purpose of CVN in a card not present transaction is to attempt to verify that the person placing the order has the card in their possession. Requesting the CVN during an online purchase does add a measure of security to the transaction. However, some survey respondents revealed that they have seen these numbers being used by fraudsters.

The results show that manual review remains a firm favourite – coming in only just behind CVN in terms of its popularity. In what should be a highly automated sales channel, 61% of merchants are still manually checking orders.

AVS is the third most popular anti-fraud tool amongst UK respondents and comes top in the US survey. However, it is subject to a significant rate of false positives which may lead to the rejection of valid orders.¹ Since AVS only checks numeric data in a street address and postcode, an AVS ‘no match’ response is not uncommon. Furthermore, AVS only covers certain markets and may not be of much assistance to businesses who are looking to expand overseas. Merchants should not rely solely on the AVS result to accept or reject an order.

It is worth noting that most merchants employ a toolkit approach, using on average four different tools to fight online fraud. This figure is also reflected by the results of the US survey. Typically, the longer a fraud prevention tool or tactic has been in place, the more likely fraudsters are to be able to establish ways of defeating the system. Merchants need to employ additional methods of identifying and managing suspicious orders to offset the impact of fraudster sophistication.



Chart 5

¹ CyberSource analysed 12.9 million credit card transactions where AVS was used and the final status of the transaction was known. If a merchant were to reject orders based solely on AVS ‘no match’ they would incorrectly reject 25% of good orders and fail to detect 61% of the fraudulent orders.

Most manually reviewed orders accepted, but at a price

The 2005 survey has highlighted that almost one in five (19%) of all merchant's orders are referred for manual checking. Of the transactions manually reviewed, a large proportion of companies go on to accept the majority of suspect orders (69% of merchants ultimately accept 80% or more of such orders), offering further indications of a wasted, or at least disproportionately costly, order verification process (Chart 6).

Furthermore, merchants that are relying on manual review may be putting a significant strain on resources. Around two in five organisations (38%) review less than ten orders per hour manually. The US survey recorded an average of just ten transactions per hour; merchants with review rates this low should examine how efficient their manual checking process really is.

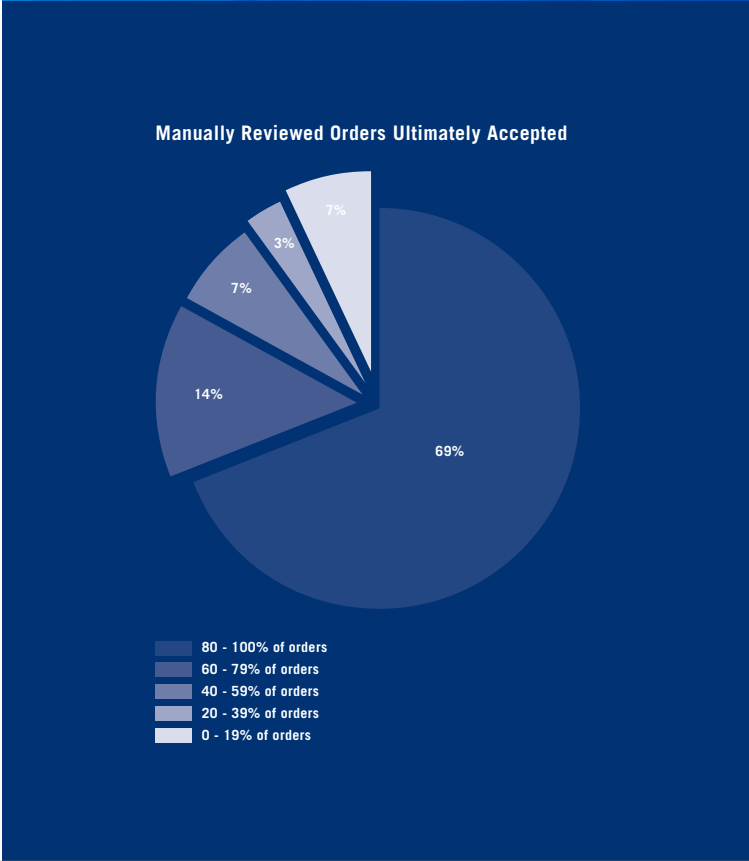
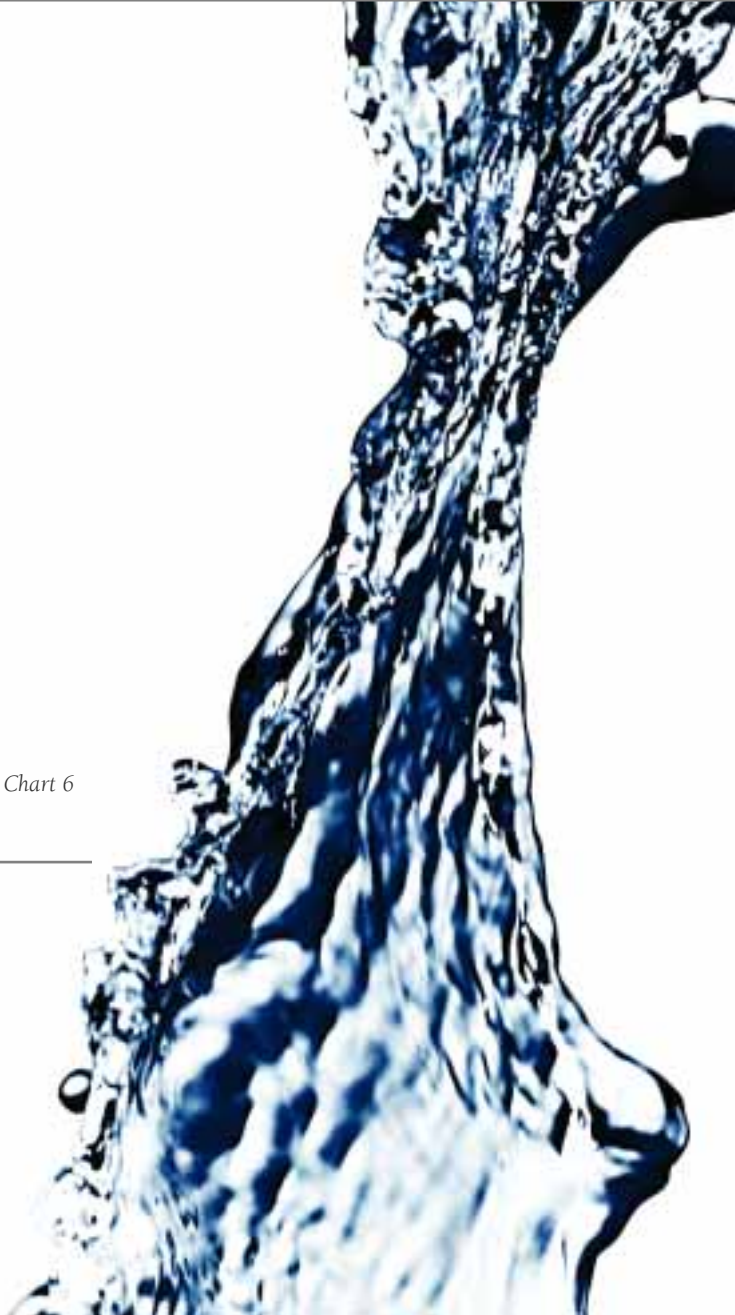


Chart 6



Manual review may be a viable process step for smaller merchants with low order volumes, but it is not normally a cost-effective or scalable solution for larger merchants with high order volumes or seasonal order peaks. Businesses that manually check significant portions of orders may need to divert more staff time to the order review process, increase staffing levels, allow more time to process orders or work to improve methods of identifying risky orders.

The problem with relying on manual review goes beyond the issues of scalability and cost, as intervention techniques often involve re-engaging the customer (Chart 7). Direct customer contact is by far the most popular method; however, this additional exchange could result in increased consumer dissatisfaction and order delays.

Manual Review Techniques in 2005

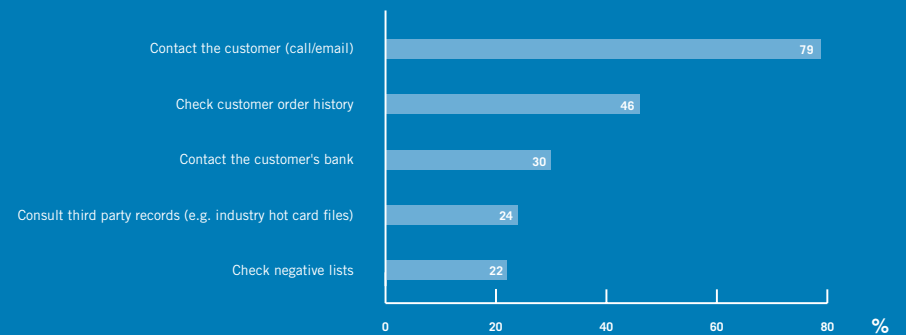


Chart 7

managing *online* fraud in 2006

Merchants' upbeat on growth - massive revenue increases forecast

On average, the businesses surveyed expect their online divisions to generate around £9.52 million in revenues during 2005 – the highest being in excess of £60 million.

Further encouragement came from the growth predictions for 2006. Just 5% of respondents forecast that their sales would remain static over the next year.

Incredibly, 95% of merchants said that they expect to see an upturn in online sales in 2006, with 36% forecasting growth of up to 20%, more than a third predicting growth of between 20% and 50% and, particularly encouragingly, almost a quarter (23%) expecting massive increases of 50% plus (Chart 8).

Online Sales Expectation for 2006

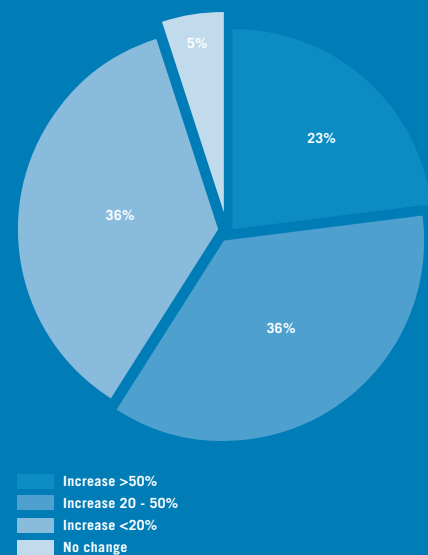


Chart 8

Implementation of authentication systems planned

Payer authentication schemes - such as Verified by Visa and MasterCard SecureCode - continue to grow in acceptance, being cited as the tool that merchants are most likely to adopt in 2006 (Chart 9).

Implementing these systems can eliminate or reduce exposure to online fraud loss by authenticating the buyer's identity or by shifting fraud liability back to the card issuing bank. Over the next few years, the schemes may help to reduce the incidence of online fraud if a critical mass of consumers register their cards and accept the new checkout procedures. Merchants will still need to have processes in place to handle customers who have not adopted the new systems or who use cards that are not yet supported.

Chart 9 reveals that a number of merchants are not planning to introduce any new anti-fraud measures during the next year (34%). This could suggest a growing confidence in current systems but may overlook new tools that aim to identify more fraudulent transactions whilst protecting good customers. Considering the previously noted worry over the increasing sophistication of fraudsters, merchants may be at risk of becoming complacent rather than actively working to address evolving fraud patterns.

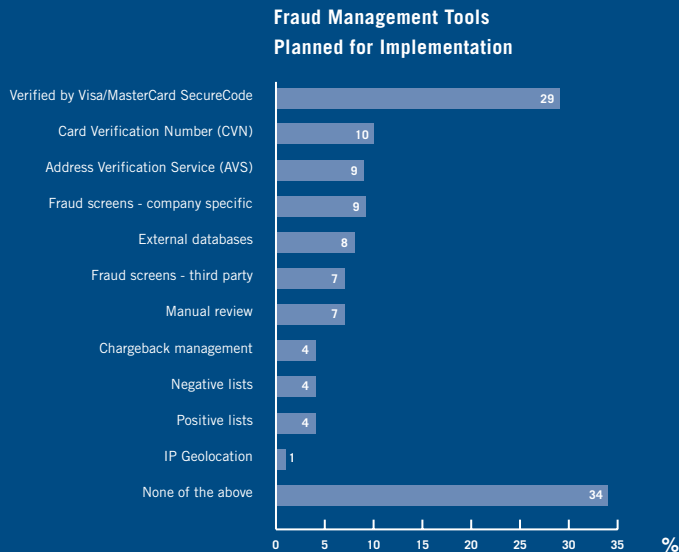


Chart 9

Little change expected in order review staffing

Over a quarter of respondents (27%) forecast that their manual review staffing levels will rise to some degree over the next year, leading to increased employee costs (Chart 10). The majority (63%) expect their staffing levels to remain static in 2006 – indicating that companies may be gaining in review confidence and efficiency (Chart 10). A word of caution however; merchants should carefully consider whether they will be able to sustain a reliance on manual review given the predicted increases in transaction volumes.

Manual Review Staffing Levels for 2006

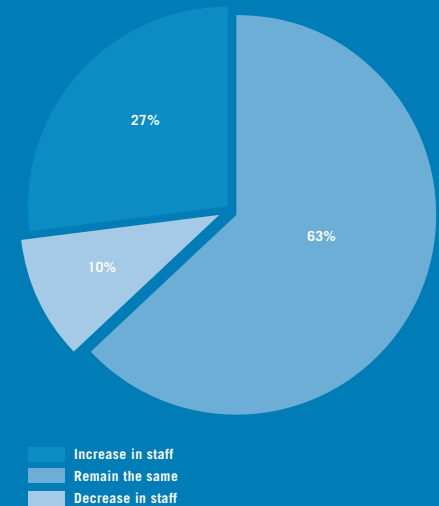


Chart 10

conclusion

It is instructive to note, at this point, that the overall cost of fraud remains far higher for bricks and mortar, high street-based businesses than it is for online, 'clicks and mortar' merchants.

Although online fraud continues to rise in gross financial terms, for many merchants it appears to be reducing as a proportion of total online spend. One might even venture that the problem is decreasing in real terms for these companies – with more and more money being spent online, and more and more transactions, but less of them turning out to be fraudulent.

Such merchants could justifiably claim to be stemming the tide where online fraud is concerned. The irony is that this means organisations, now more than ever, need to be on their guard. Keeping fraud at bay is as important in the current climate as it has been at any other time. Accordingly, merchants must maintain their focus and their investments in anti-fraud measures if they are to avoid falling victim to the increasingly sophisticated techniques of online criminals.

Now though, the agenda is moving on. Forward-looking online businesses are already beginning to view anti-fraud technologies differently; to use them as more than just precautionary tools – as technologies that can empower greater efficiencies, competitive edge and customer satisfaction.

However, for this to happen fully, the anti-fraud industry must look to evolve its role beyond the fear, uncertainty and doubt-based messages which have often been promoted.

Merchants too must continue their evolution and keep investing in strong anti-fraud measures, protecting eCommerce operations alongside other sales channels. After all, those who commit fraud will ultimately react in much the same manner as anyone else that is forced to take a pay cut. They will look for a new 'job', finding new sales channels to exploit – those with the greatest real or perceived weaknesses and without the robust defences to protect themselves.

Organisations that play down the intensity of their anti-fraud planning and provisioning should take heed. Whilst the threat of online fraud may be waning for some merchants, there is nothing to indicate that it has dissipated in any lasting or long-term way.

for more *information*

Call +44 (0)118 965 3819

Email uk@cybersource.com

Visit www.cybersource.com

Risk Management Solutions

Efficiently managing online fraud involves integrating multiple tools and technologies to maximise operational efficiency and sales conversion, while minimising fraud risk.

CyberSource's modular, scalable solutions are designed to meet these objectives and help you achieve superior results. Our solutions can be quickly and easily implemented as a single component or as fully-integrated systems and can be managed in-house, outsourced or constructed as a blend of both.

Managed Service - *CyberSource Managed Risk Service*

This service provides the complete professional analysis, design, modelling and monitoring services required to optimise transaction conversion, whilst minimising manual review and fraud risk for card not present transactions. We collaborate with you to set business metrics, review performance and provide easy-to-use business tools, such as CyberSource Decision Manager, that let you control as much or as little as you wish.

Rule and Decisioning Systems - *CyberSource Decision Manager*

CyberSource offers a range of cost-effective, easy to implement decision management systems that allow you to control all fraud tools and set rules for order acceptance via one easy-to-use 'dashboard', with no IT coding required. The systems include interfaces to

About CyberSource

CyberSource Ltd. is a wholly-owned subsidiary of CyberSource Corporation. CyberSource is a leading provider of electronic payment and risk management solutions. CyberSource solutions enable electronic payment processing for Web, call centre, and POS environments.

CyberSource also offers industry leading risk management solutions for merchants accepting card not present transactions. CyberSource Professional Services designs, integrates, and optimises commerce transaction processing systems. Approximately 12,000 businesses use CyberSource solutions, including half the companies comprising the Dow Jones Industrial Average. The company is headquartered in Mountain View, California, and has sales and service offices in Japan, the United Kingdom, and other locations in the United States. For more information, please visit CyberSource's website at www.cybersource.com or email uk@cybersource.com.

advanced fraud scoring technology as well as other external services and your own data.

Based on your business rules the systems automatically tag the order as accept, reject, or review, helping you to accept more valid orders and reject more fraudulent ones.

Verified by Visa/MasterCard SecureCode - *CyberSource Payer Authentication Service*

This service allows you to minimise online card fraud and customer disputes, receive repudiation chargeback protection and obtain relief from fraud liability. You receive the online payment guarantees offered by Verified by Visa and MasterCard SecureCode, all with the ease of a single connection to CyberSource.

Payment Solutions

CyberSource Payment Service

CyberSource offers secure, reliable real-time payment processing in multiple currencies worldwide. Our payment solutions support global payment types including universal and country specific credit/debit cards, bank transfer, direct debit and ELV.

Complementary services include PayPal, delivery address verification, tax calculation and PCI Compliance.

Europe

CyberSource Ltd.
400 Thames Valley Park Drive
Thames Valley Park
Reading RG6 1PT
United Kingdom
T: +44 (0)118 965 3819
F: +44 (0)870 460 1931
E: uk@cybersource.com

North America

CyberSource Corporation
1295 Charleston Road
Mountain View
CA 94043
USA
T: +1 650 965 6000
F: +1 650 625 9145
E: info@cybersource.com

Japan

CyberSource KK
3-25-18 Shibuya
Shibuya-ku
Tokyo 150-0002
Japan
T: +81 3 4363 4111
F: +81 3 4363 4118
E: mail@cybersource.co.jp

Founded in 1995, CyberSource pioneered online fraud screening at the inception of internet commerce. Today, our payment processing and risk management solutions have set the standard for the industry, with CyberSource becoming the trusted provider to thousands of businesses worldwide.

www.cybersource.com
www.thepowerofpayment.co.uk

CyberSource®
the power of payment