CyberSource®
the power of payment

Sixth Annual

UK ONLINE FRAUD REPORT

2010 edition

Online Payment Fraud Trends,
Merchant & Consumer Response

Methodology

For the sixth consecutive year, CyberSource presents the UK Online Fraud Report; the most comprehensive study of online fraud in the UK. For this latest edition we've surveyed more merchants – now over 200 – and added further in-depth analysis of the results. Included within the report is best practice advice for businesses trading online, as well as industry comments from Visa, MasterCard and a Detective Superintendent of the Metropolitan Police.

Working with Vanson Bourne, a specialist technology-industry research consultancy, CyberSource has developed a consistent and independent survey of UK-based merchants. Through online and telephone research, CyberSource has gained valuable insight from respondents either directly responsible for, or having influence over, online fraud policy and decisions on the management of fraud. They revealed details about their revenues and expenditure, their operations, and most importantly their experiences with fraud and how they defend themselves against crime. The analysis of these responses provides insight into how fraud is impacting the overall eCommerce industry.

For the third year, retail and technology market research expert, Gfk NOP, spoke with over 1000 consumers to learn more about their experiences of online fraud and their understanding of the problem. We introduced new questions to further understand their concerns, consider the impact of online fraud on consumers and identify new opportunities for merchants.

This year, CyberSource has changed the format of the Fraud Report to represent an end-to-end view of the risk management process, from automated screening, through to manual review, order dispositioning, and fraud claim management. The report highlights where profits can be lost, and also shows how best to protect businesses against these risks. Presented throughout is a selection of the most fascinating data, along with analysis of the key trends.

Co-Authored by Dr Akif Khan, Head of Client and Technical Services, CyberSource

As Head of Client and Technical Services, Dr Akif Khan has continued to elevate his thought-leadership status throughout the eCommerce industry. A sought after consultant and speaker within the online fraud arena, he helps and advises online businesses all over the world. Dr Khan has witnessed the latest challenges faced by organisations in multiple geographies and market sectors.

Over the last twelve months, Dr Khan has helped initiate a new approach to payment security; counselling merchants across the globe on the latest ways to not only defend against fraud, but to keep data protected.

This year, Dr Khan has provided consultancy throughout the report, as well as advising on the next generation of fraud tools, staging for economic recovery and the development of mobile payments.

Table of Contents

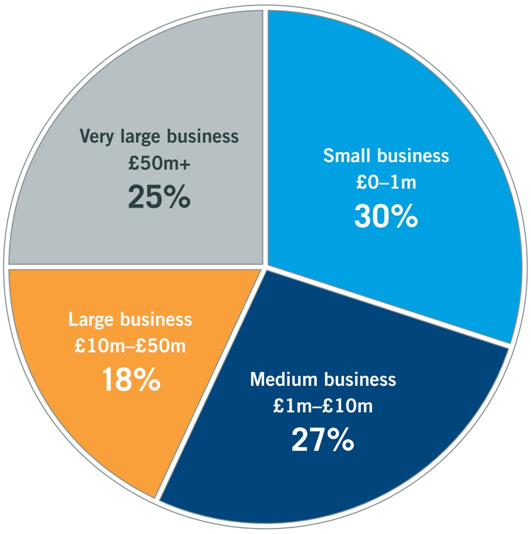
The Survey Base; Today's UK Online Business

To provide some context to the 2010 report, merchants were asked a series of questions about their business and the impact of online payment fraud. Looking at online revenue, the proportion of companies responding from each band remained relatively similar to the previous survey. There was a reasonably even split between respondents from small businesses (£0-1m online revenue), medium-sized businesses (£1m-£10m), and very large businesses (£50m+). The smallest group of respondents came from large organisations (£10m-£50m), at 18% (Chart 1).

Respondents covered a wide range of business sectors (Chart 2). Almost half of the merchants surveyed (49%) were retailers of physical goods e.g. clothing, books/DVDs, health and beauty, office supplies etc. The remaining respondents were split relatively evenly between services (including consumer finance, payment services, education, government), travel (such as travel agencies, tour operators, travel portals, hotels, car rental/rail/cruise specialists), and digital goods (including online news, publishing, online games, social networking, downloaded music/movies, communications/internet providers, tickets).

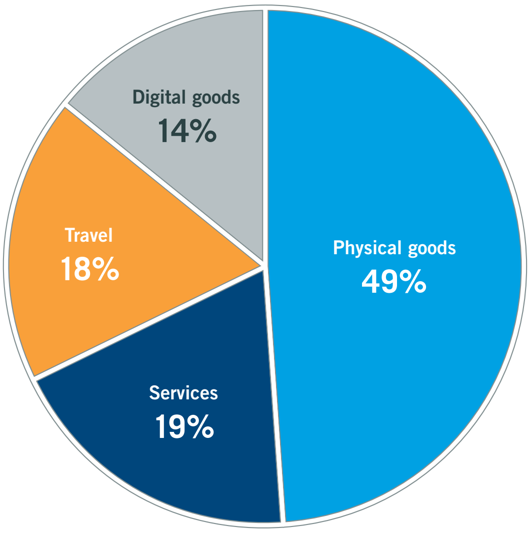
Respondent Company Sizes by Online Revenue

1



Respondent Company by Market Sector

2



Executive Summary

Managing online fraud continues to be a significant and growing cost for merchants of all sizes. To better understand the impact of payment fraud for online merchants, CyberSource sponsors annual surveys addressing the detection, prevention and management of online fraud. This report summarises findings from the sixth annual UK survey.

Economic Impacts of 2009 and Optimism for 2010

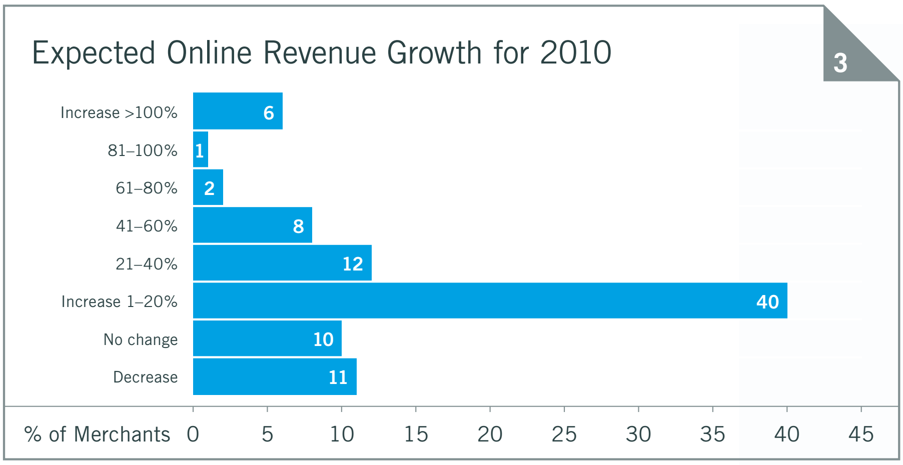
The previous UK Online Fraud Report highlighted that just 51% of merchants were forecasting growth for their companies in 2009. In actual fact, even amongst the financial turmoil of late, the latest survey found that 68% of respondents were predicting an increase in their 2009 annual online revenue; only 18% of respondents were forecasting a fall. The survey results show that small to medium sized businesses (with online revenues of £0-10m) were experiencing higher growth rates than some of the larger, well established, online retailers. When examining all respondents, nearly one-third predicted an increase in their 2009 online revenue of up to 10%; this is an impressive figure given the environment in which businesses are operating.

Looking to the future, merchants are more optimistic about 2010, with 69% expecting online revenues to grow year-on-year; 11% anticipate a decrease. Once again, the smaller companies, with lower online revenues, are even more optimistic; the average expected increase is double that of the larger businesses.

Overall, 40% of merchants are predicting an increase in online revenue of up to 20% in 2010, with just under a third expecting growth of 20% or more (Chart 3)[1]. On balance, this indicates increased optimism for 2010, particularly given that actual online revenue growth rates tend to be higher than those disclosed at the time of the survey. In 2007, 80% of businesses were forecasting online revenue growth; these latest results show that confidence is once again improving. As companies look to stage their recovery from the economic crisis, online retail will continue to be a source of growth for merchants.

Impact of Fraud

One-third of businesses are seeing the percentage of online revenue lost to fraud increase year-on-year, whilst just under half of merchants are observing a decline or no change. Overall, merchants expect to lose an average of 1.8% of their overall online revenue to payment fraud; this represents an average of £400,000 in lost revenue across all sizes of business for 2009. That being said, 48% of merchants expect to lose less than 1% of their 2009 online revenue to payment fraud.



[1] Chart 3: 10% of the survey base responded 'Don't know'.

Greatest Business Threats

We asked merchants to rank the greatest threats to their business and, for the third year running, online fraud (57%) was rated as one of greatest business threats (Chart 4). One of the most dramatic changes over the years has been the increased awareness and concern about the theft of customer data. In 2007, just 6% of merchants ranked it as a serious threat – over the past two years this figure has jumped to over half of merchants.

The latest survey reveals that large and very large businesses are the most concerned about the threat of data theft (60%). This is potentially explained by the impact that data theft has had on a number of high profile brands; many were storing a lot of customer data by virtue of their size. Implementing a payment security strategy to secure sensitive payment and personal details is more important than ever before to help protect customers, brand and revenue.

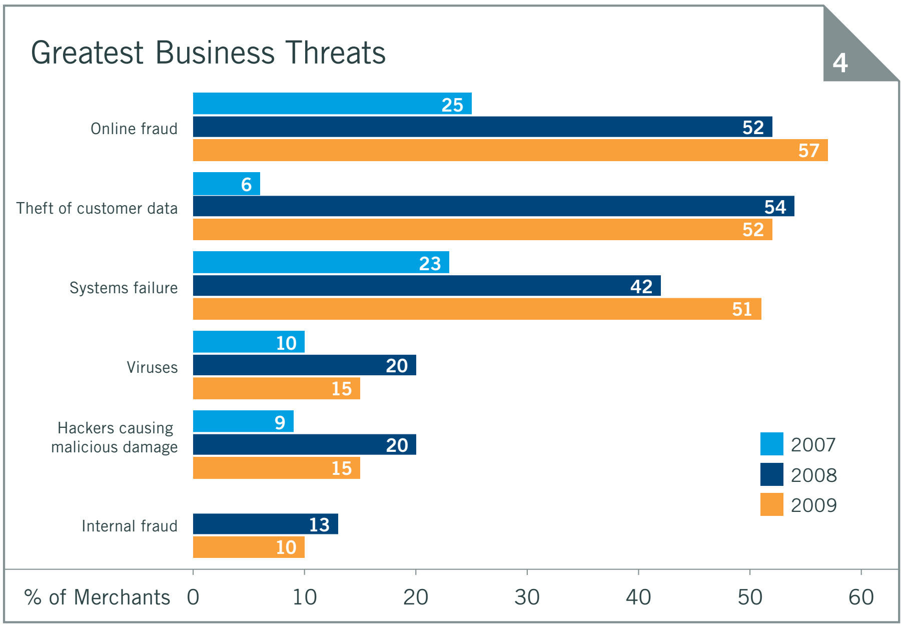
Payment and Fraud Management Trends

Credit and debit cards remain three times more popular than other payment acceptance methods. For the third consecutive year, the popularity of the 3D Secure schemes, Verified by Visa and MasterCard SecureCode, has continued to grow. Merchants are increasingly using these programmes (in part due to the Maestro mandate) to help protect against fraudulent transactions and the costs associated with them.

Over 70% of merchants manually review orders as part of their fraud management process, with 5% manually checking every order. Manual review can be very time and cost intensive, especially given that more efficient automated screening tools could improve throughput. While this method has its place, automated systems should generally be used as the first line of defence, with reviewers only checking those orders flagged by the system as warranting further investigation.

Responsibility for Safer Shopping

Half of UK consumers still do not shop on the web and, overall, 71% are concerned about the safety of online shopping. Friends, family and the media continue to exert influence over consumers using the internet. When the consumer fraud survey was first conducted in 2007, we asked who should be held primarily responsible for making online shopping safer. The prevailing opinion was that retailers should take ownership. Two years on, we asked consumers the same question. Interestingly, the top answer was still retailers, yielding exactly the same percentage response as before – 24% of respondents felt that retailers were primarily responsible for making online shopping safer.



Setting the Scene

Since the first UK Online Fraud Report in 2005, we have recognised changes in the way merchants approach the management of online fraud. In an ever-evolving world, businesses are required to adapt to meet the demands of consumers, such as offering their preferred payment types, whilst also implementing new fraud tools and techniques that address the latest threats.

Plastic Cards Reign

Credit and debit cards remain the most popular form of payment acceptance, with 96% of respondents offering this method. A third of merchants stated that they accept payments in currencies other than GBP. There has been an increase in merchants accepting country and region-specific cards outside of the UK, such as Carte Bleue, probably due to businesses looking abroad for additional online revenue opportunities.

PayPal continues to be a prominent payment contender, with 32% of merchants accepting this method, while Google Checkout remains stagnant at 9%. Bank transfers are accepted by 31% of merchants, whilst direct debit has slipped from 33% in the previous survey to 17% this time around. Finally, whilst the percentages are low, 4% of respondents say that they accept payments via mobile phone.

Expansion High on the Agenda

Regional and global expansion presents real opportunities for online growth – something that UK merchants are keen to embrace, particularly in the current economic climate. This is played out by the survey results, which reveal that a large number of respondents already sell into Europe, the Americas and Asia Pacific (APAC).

Indeed, France, Germany, Italy and Spain are each served by over half of the merchants that accept international orders. A relatively high proportion of UK merchants (49%) accept orders from the US, whilst 38% serve Canada, and 24% serve Mexico and Brazil respectively (Chart 5, overleaf). Within APAC, Australia stands out as the country that most merchants accept orders from (35%).

We also looked more specifically at the countries that UK merchants were planning to accept orders from over the next 12 months. Interestingly, the top three are China (14%), and two Latin American countries, Brazil (13%) and Mexico (13%).

It is worth noting that the APAC region represents a significant growth opportunity for merchants – similar to the UK, plastic cards are the preferred payment method in a number of APAC countries, plus consumer adoption of the online channel is also rapidly increasing within this region.

BEST PRACTICE
advice

Approaching Global Fraud Management

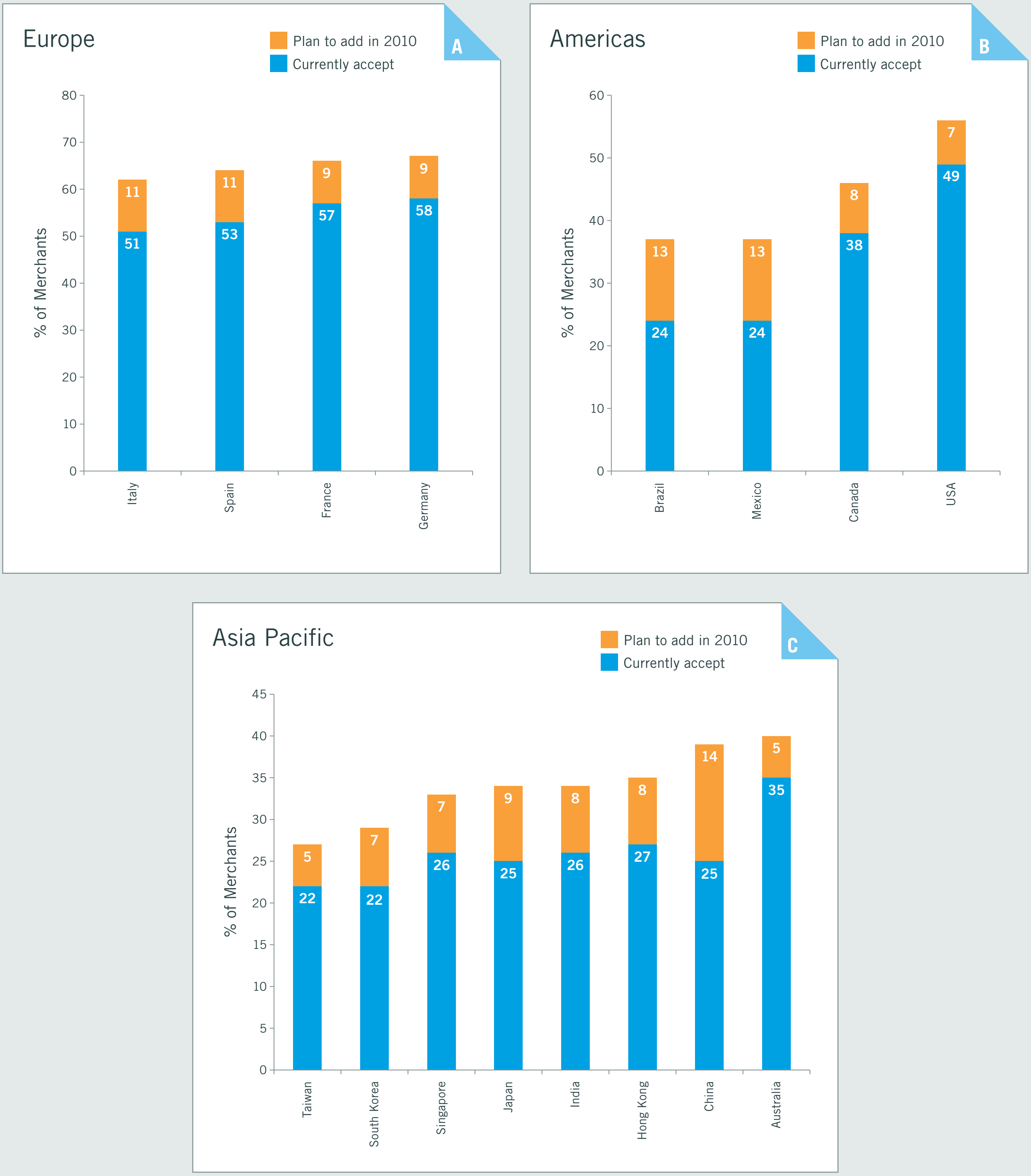
Whilst there are some universal principles that can be applied to the acceptance of online orders, merchants should note there are a number of key differences that need to be considered to help keep fraud losses in each territory at bay. Geographical expansion presents additional fraud and payment challenges, but by offering the right payment type for the right product, understanding the national laws, regulating consumer transactions and being mindful of language barriers, merchants can thrive.

Businesses should look to review their existing fraud screening strategy to ensure that their tools are not only optimised for the countries into which they are selling, but for their particular sector and offering. A rules-based system can be used to help ensure that such regional and product line differences are incorporated into a merchant's fraud screening methodology. The system should be flexible enough to allow rule updates to be made in real-time by the merchant, and not by IT. In doing so, merchants can easily fine-tune business rules specific to a geography, changing them as often as they need to.

Furthermore, it is vital for merchants to ensure that their manual review team is familiar with the local shopping environment for the countries into which they are selling. This will help them more easily spot formatting errors in addresses, as well as risky correlations between billing and shipping towns.

% of Merchants Accepting International Orders

5



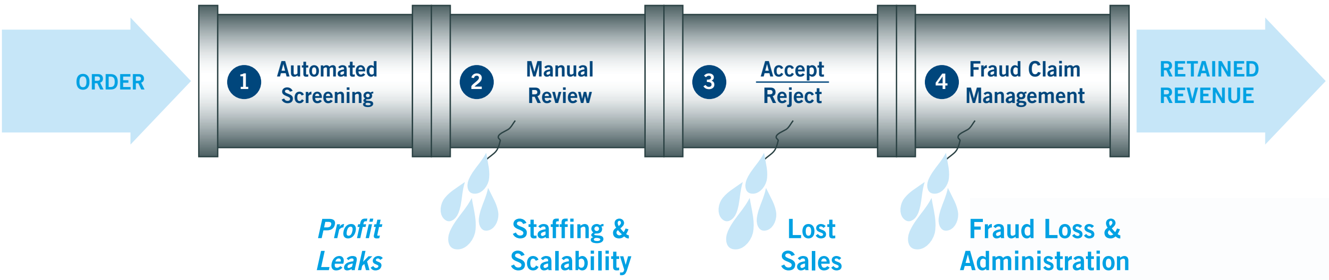
Total Pipeline View Required

Organisations that focus solely on managing chargebacks may not be seeing the complete financial picture. Online payment fraud impacts profits from eCommerce sales in multiple ways. Besides direct revenue losses, the cost of stolen goods/services and associated delivery/fulfilment costs, there are the additional costs of rejecting valid orders, staffing manual review teams, administration of fraud claims, paying for the maintenance of internal systems and the cost of using third party tools. In addition to these costs, there is also the challenge associated with business scalability. Merchants can gain efficiency by taking a total pipeline view of operations and costs. While the fraud rate is one metric to monitor, an end-to-end view is required to arrive at the best possible financial outcome.

A Risk Management Pipeline is used to illustrate some of the profit leaks that take place throughout the payment process. One-third of merchants report that the percentage of online revenue lost to payment fraud has increased year-on-year. Looking in more detail at the data, it is evident that merchants are rejecting 4.6% of incoming orders due to suspicion of fraud. Whilst larger companies report that they reject a marginally higher number of orders due to suspicion of fraud, they also receive a higher proportion of fraudulent orders.

Merchants report that they are manually reviewing 18% of orders, and yet 69% are ultimately accepted. Overall, 1.6% of accepted orders later result in fraud losses. The 2010 UK Online Fraud Report details key metrics and practices at each point in the Risk Management Pipeline in order to provide benchmarks and additional insight for businesses trading online.

Risk Management Pipeline



Merchants review, on average, 18% of orders (a decrease of just 1% since the last report)

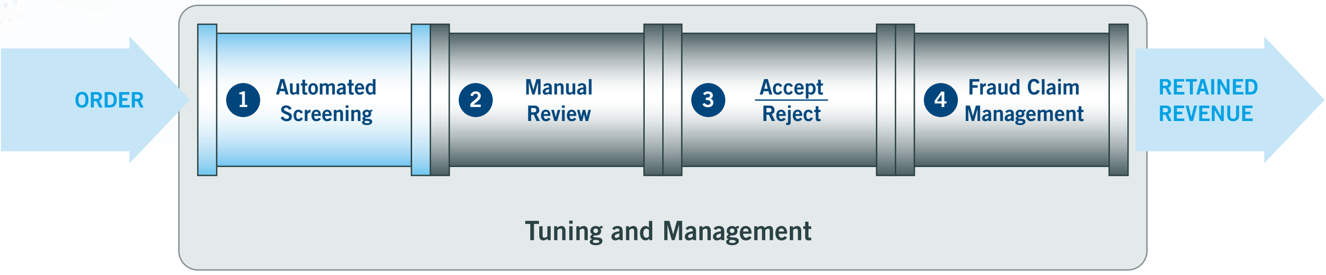
On average, merchants reject 4.6% of orders – some may be valid

69% of reviewed orders are ultimately accepted (a decrease of just 3% over the previous report)

1.6% of orders overall prove to be fraudulent

23% of chargebacks are fraud reason-coded

Stage 1: Automated Screening



Automated Fraud Screening in Practice

Detection tools are those used to identify the probability of risk associated with a transaction or to validate the identity of the purchaser. Results of tests carried out by detection tools are then interpreted by reviewers or rules systems to determine if a transaction should be accepted, rejected or reviewed. A wide variety of tools are available to help merchants evaluate incoming orders for potential fraud.

Merchants handling large online order volumes typically employ an initial automated order evaluation system, either internally or from a vendor, to determine if an incoming order might represent a fraud risk. Some merchants will allow this automated screen to reject orders without further human intervention. Indeed, in the equivalent survey carried out by CyberSource in the US, 47% of merchants said that they cancelled some orders as a direct result of their automated screening process.

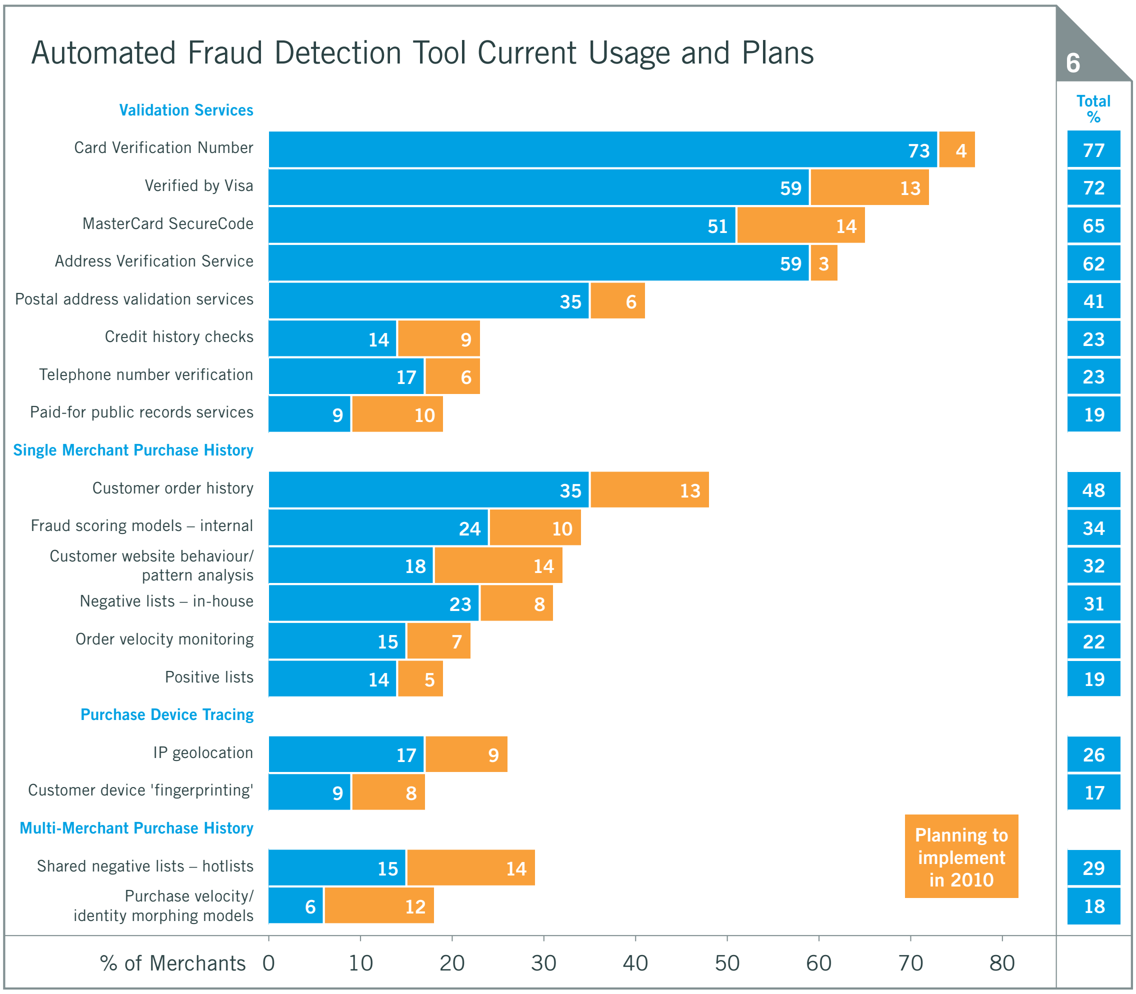
Momentum Continues for Verified by Visa and MasterCard SecureCode

For the third year running, the popularity of the 3D Secure schemes, Verified by Visa and MasterCard SecureCode, has continued to grow (Chart 6). The password-protected identity verification services help to mitigate the risk of online fraud for merchants. In adopting the programmes, merchants can receive protection from fraud-related chargebacks, as liability for qualifying transactions is transferred from the merchant to the card-issuing bank. Used in isolation, the 3D Secure schemes will not be completely effective, but by combining them with other fraud screening tools, merchants can minimise the cost of fraud to their business.

Address Verification Service (AVS) and Card Verification Number (CVN) continue to be used heavily by merchants. Again, AVS and CVN should not be used in isolation. More specifically, AVS is subject to a significant rate of ‘false positives’, which may lead to merchants unnecessarily rejecting valid orders as well as accepting fraudulent ones. If the cardholder has a new address or a valid alternate address, this information may not be reflected in the records of the cardholder’s issuing bank, so the address would be flagged as invalid.

The purpose of CVN in a card not present transaction is to attempt to verify that the person placing the order has the actual card in his or her possession. Requesting the CVN during an online purchase can add a measure of security to the transaction. However, fraudsters have demonstrated that they can obtain CVN numbers, as evidenced by their availability for sale online.

The smallest online merchants are less likely to use 3D Secure schemes, AVS or CVN. They are also less likely to utilise the next two most popular methods; customer order history and postal address validation services. Larger online businesses make much greater use of the most popular fraud detection tools.


Automated Fraud Detection Tool Current Usage and Plans

Investment Planned in Automated Screening Tools

Merchants continue to invest in fraud management methods. Today it is standard practice to deploy multiple tools – merchants typically employ between five and six different anti-fraud tools. Large or very large businesses use an average of seven tools as part of their automated screening process. Significantly, 70% of companies plan to introduce additional fraud systems in 2010. The top tools planned for implementation in 2010 are the 3D Secure (also known as payer authentication) schemes, Verified by Visa and MasterCard SecureCode, website behaviour analysis and making better use of negative lists.

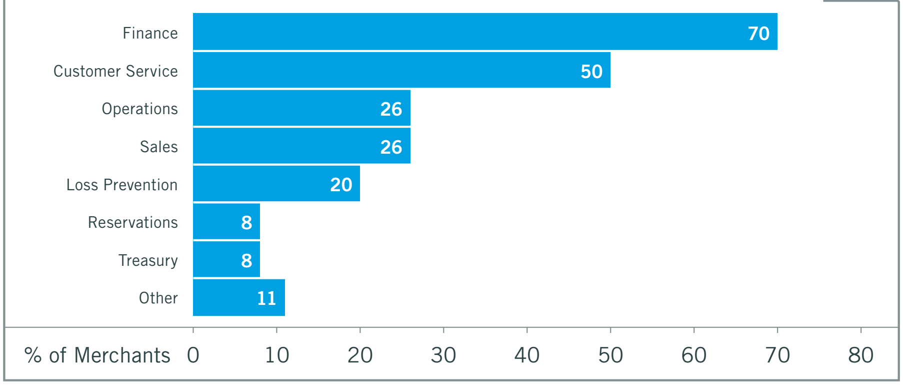
Interestingly, the tools that most merchants plan to adopt in the US are device printing (27%), IP geolocation (22%) and payer authentication (20%). In the UK, just 8% of respondents plan to invest in device fingerprinting. This anti-fraud tool is one of the more recent to appear; it examines and records details about the configuration of the device from which the order is being placed. This can aid in flagging fraud attacks where a variety of fraudulent orders are launched from a common device or set of devices.

Payment Security: Different Approaches Being Adopted

The theft of customer data remains one of the top threats to merchants' businesses. Given the damaging effect that this can have on an organisation's reputation, it is more important than ever to protect payment information against internal and external threats.

In today's complex merchant environments, sensitive payment data is often spread across the entire organisation. Data may be stored throughout the end-to-end payment process – for instance during its initial capture, on databases, and for the purposes of manual review and chargeback management. As a consequence, multiple departments and employees may have access to this sensitive information (Chart 7), potentially increasing the risk of data theft or exposure.

Departments with Access to Customer Payment Data



A common approach to managing data is to 'lock it down' – this focuses on encrypting payment data within merchants' environments. However, this approach has challenges; it requires merchants to know precisely where all payment data resides and how it flows within the organisation. In addition, the ongoing costs and resource overhead of key management, as well as ensuring new systems fit into the encryption paradigm, can make the business case problematic. Alternatively, rather than handling the data themselves, a number of organisations are now opting to remove all payment data interaction within their environment. For example, payment data storage can be eliminated by using remote tokenisation services, whilst some merchants, both large and small, may select hosted payment acceptance, which eliminates data capture by their systems.

INDUSTRY comment

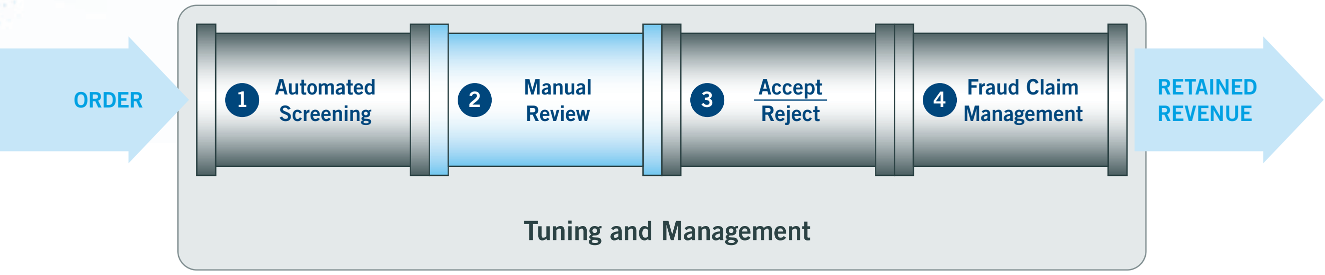
MasterCard SecureCode is a global eCommerce solution that adds an additional level of security to online shopping. It continues to gain rapid acceptance, with more than 400,000 merchants worldwide offering this secure online payment service.

Even though fundamental security needs are the same across the industry, individual business needs, processes, and solutions differ. MasterCard recognises these unique requirements and places a premium on flexibility. That is why SecureCode enables issuers to choose from a broad array of security solutions for authenticating their cardholders, including password or smart card-based approaches. MasterCard also actively works with issuers globally to examine new methods of authenticating cardholders during the SecureCode transaction, providing the framework upon which the issuers can implement the authentication method of their choice.

While the majority of issuers currently use static passwords, there is an increasing drive in particular regions to move towards next-generation methods of authentication. These regional efforts range from dynamic passcodes generated from chip-based solutions, such as the increasingly prolific card readers used in the online banking process, to mobile services whereby an issuer could send a one-time passcode via SMS to the mobile phone of the registered cardholder.

Paul Baker
Vice President, Payment System Integrity, MasterCard Worldwide

Stage 2: Manual Review



Manual Order Review Rates Remain High

Orders which are not accepted or rejected during the automated order screening stage typically enter a manual review queue. During this stage, additional information is often collected to determine if orders should be accepted, or rejected due to excessive fraud risk.

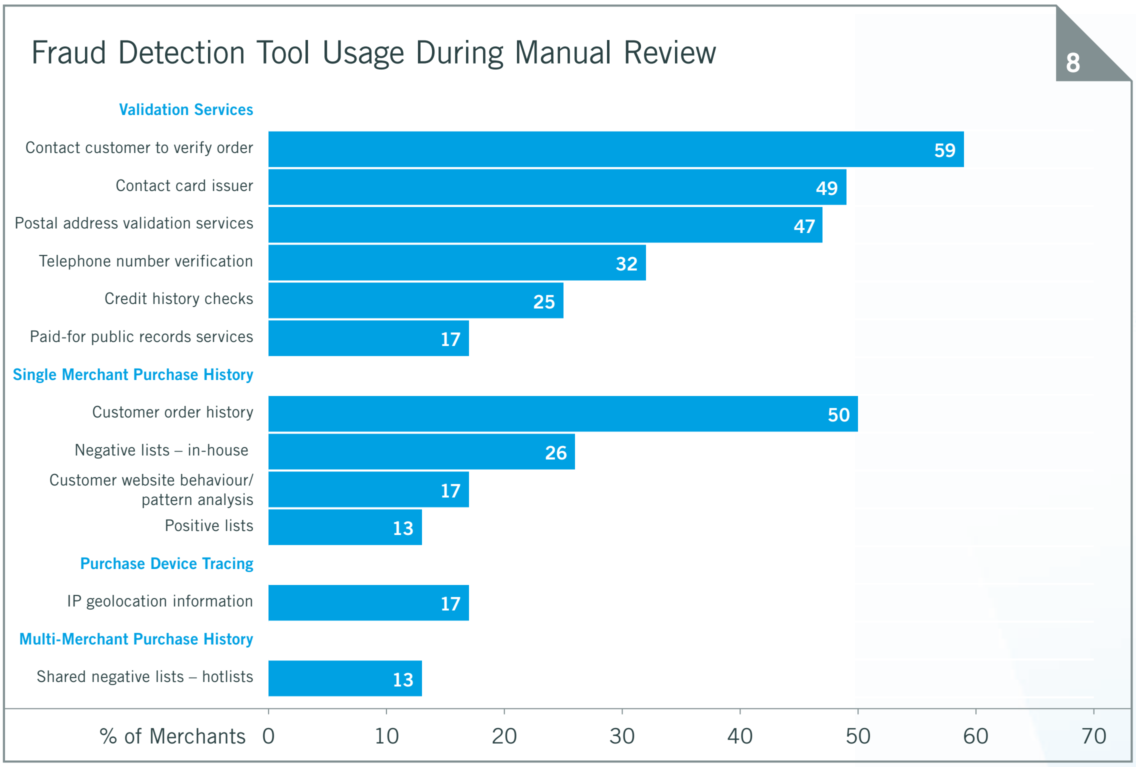
Over 70% of merchants surveyed use manual review as part of their order screening process. Five percent of merchants still manually review every order, down from 10% in the previous survey. Small and medium-sized businesses manually check two-thirds of their online orders (lower order volumes may permit such a practice).

Manual review represents a critical area of profit leakage; if not managed effectively it can be expensive, limit scalability and impact customer satisfaction.

Multiple Tools Used During Manual Review

While many of the tools or detector results used during automated screening can also be utilised during manual review, several additional tools and processes are employed by reviewers. Attempting to validate an order by contacting the customer is the most commonly used method; it is standard practice for nearly 60% of merchants utilising manual review (Chart 8). Importantly, many organisations will have policies in place regarding how quickly they must clear orders via manual review and how long they will wait for customers to respond to requests for additional information.

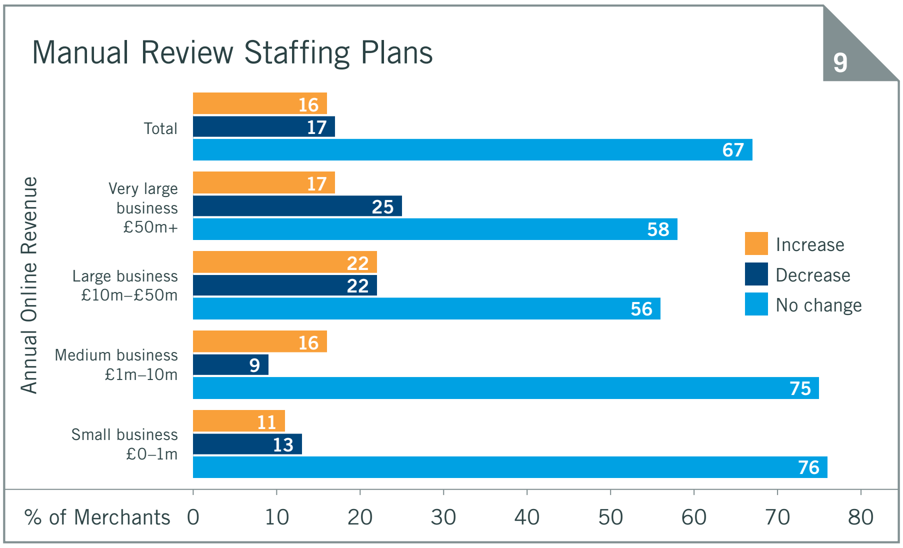
The survey found that the second most popular method is reviewing past customer order history, which is used by half of respondents overall, and 61% of very large merchants. This is followed by contacting the card issuer, an action taken by 49% of the merchants that employ manual review (versus nearly 60% of large and very large businesses). Overall, reviewers typically employ four different tools. However, for large and very large merchants this number increases to between five and six.



Greater Accuracy Required

For 68% of small businesses, each reviewer analyses less than 30 orders a day. At the opposite end of the scale, 14% of very large businesses indicated that each reviewer checks more than 120 orders a day. The results show that there is a direct correlation between the size of a company's online revenue and the number of orders each reviewer is able to analyse. Manual review teams at larger merchants may have greater throughput because they have access to more advanced case management tools. As an aside, the latest CyberSource US fraud survey found that reviewers spent eight minutes analysing each order in 2009.

On average, review teams comprise the equivalent of six full-time members, and the survey revealed that this is unlikely to alter much in 2010 (Chart 9). The vast majority of merchants are not planning to make any changes to the size of their teams. With 69% of respondents expecting an increase in online revenues in 2010, merchants' review teams may struggle to cope with greater order volumes. It is therefore important to maximise the productivity and effectiveness of review staff. While the main focus should be on improving initial automated sorting accuracy to decrease the need for review, attention should also be paid to streamlining the review process itself.



Use of Case Management Systems Increasing

The survey found that 23% of merchants currently use a case management system to support their manual review process (Chart 10). Case management systems consolidate order information, and present the results for reviewers to assess and action as required. Not surprisingly, case management systems are more widely used at large merchants (33%). It is worth noting that 27% of businesses stated that they planned to introduce a case management system in the next 12 months. Therefore, by the end of 2010, half of all merchants should have a system in place to help support their manual review process and staff.

BEST PRACTICE
advice

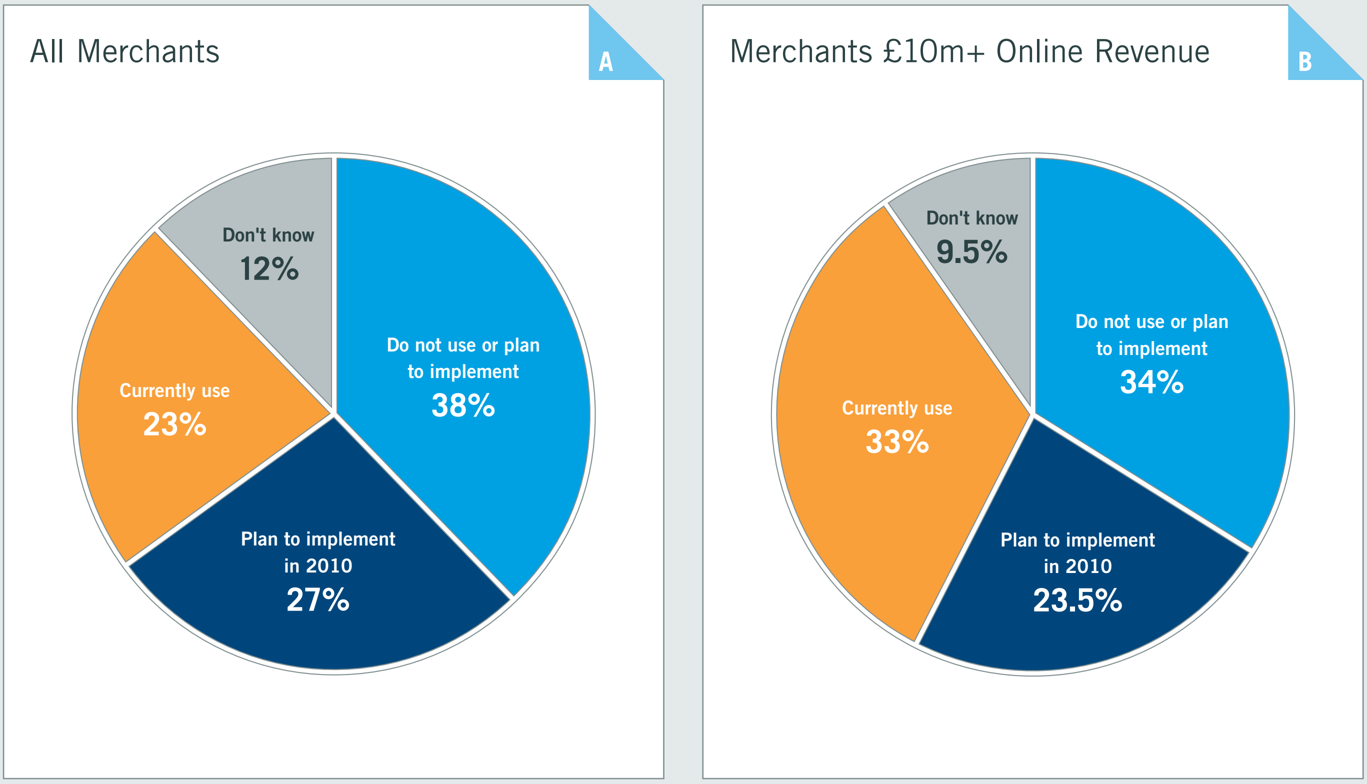
Staging for Recovery

During this period of economic uncertainty, many merchants are understandably making cost savings, and their fraud screening processes are not immune to cuts. Some merchants are finding it difficult to justify investment in updating systems or tools, as capital expenditure on new projects is being watched very closely.

Instead, the 'false economy' approach of employing more staff (often temporary workers on short-term contracts) to manually review orders is more typical. Whilst this provides an interim solution, it doesn't position the merchant well for the inevitable growth in volumes that will come as the economic recovery gathers pace. Review teams will simply not be able to cope without the appropriate systems in place to increase the amount of straight-through processing. In the meantime, fraudsters won't have been sitting back. On the contrary, their skills and tactics will have continued to evolve, and merchants need to invest in the right tools to keep pace with them or face financial losses.

Case Management Usage

10



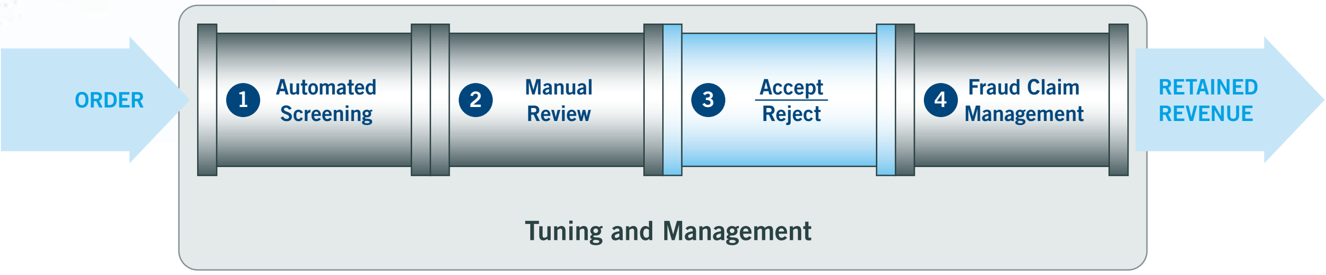
All Merchants

A

Merchants £10m+ Online Revenue

B

Stage 3: Order Dispositioning (Accept/Reject)



Post-Review Order Acceptance Rates High

Automated screening and manual order review ultimately result in order acceptance or rejection. The survey found that a high percentage of manually reviewed orders are actually accepted. Indeed, merchants who manually check orders indicated that they ultimately accept over two-thirds – this figure is similar across all sizes of business. Significantly, a third of organisations indicated that they ultimately accept over 91% of manually reviewed orders (Chart 11)[2].

Merchants are incurring significant expense to find the small percentage of the review queue they believe to be too risky to accept. Clearly, organisations need to introduce better methods to determine which orders require manual review, so that only truly suspicious orders receive this additional layer of authentication.

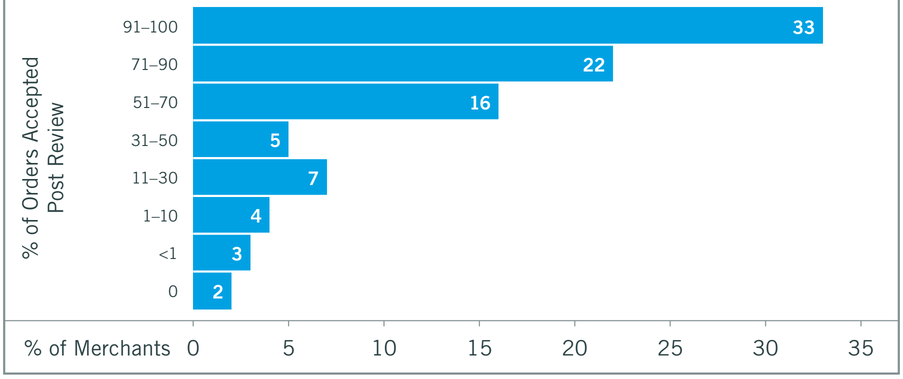
Order Rejection Rates Not Declining

Order reject rates can reflect true fraud risk or signal 'profit leaks' in terms of valid order rejection or unnecessarily high rates of manual review. As a weighted average, merchants reject 4.6% of orders due to suspicion of fraud (Chart 12)[3]. Over the last few years this figure has remained relatively consistent, and is certainly an area that needs to be addressed in 2010.

It is important to bear in mind that not all of the rejected orders will be fraudulent, representing a lost revenue opportunity for merchants. Poor fraud screening, over-cautiousness and lack of expertise could all be contributing to these high rejection rates. It remains to be seen whether merchants can decrease their overall order rejection rates without an increase in fraud rates or manual order review.

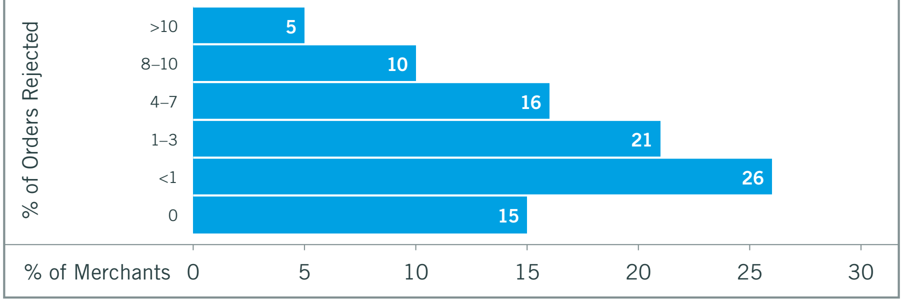
Post Manual Review Acceptance Rates

11



% of Orders Rejected Due to Suspicion of Fraud

12



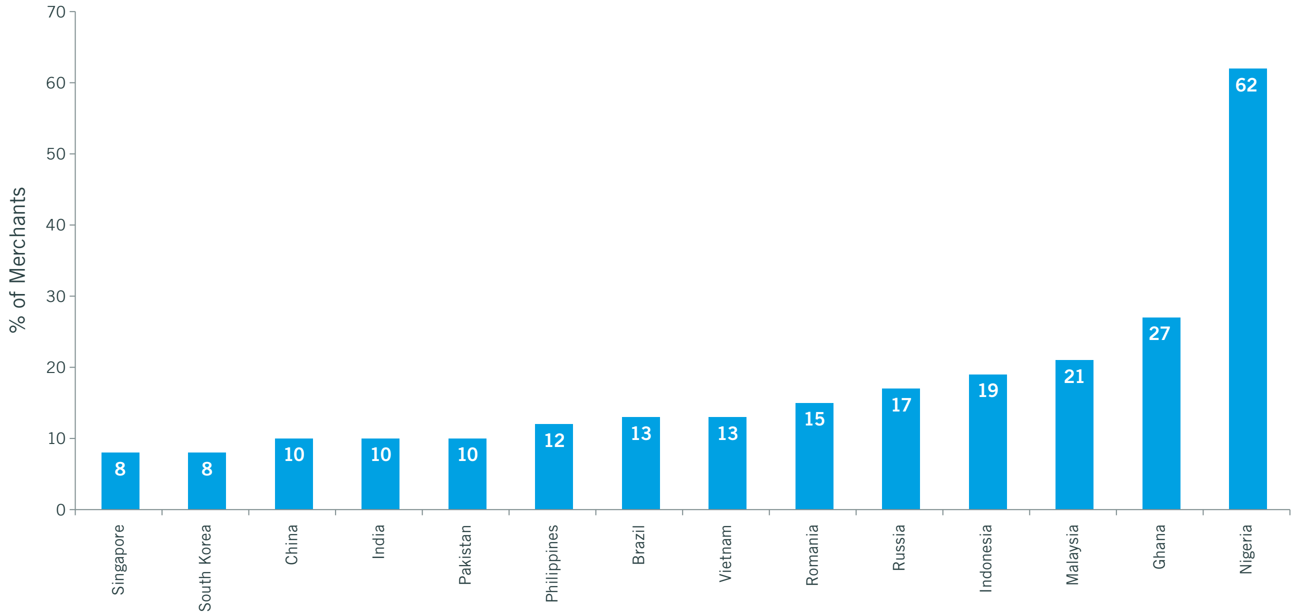
[2] Chart 11: 8% of the survey base responded 'Don't know'. [3] Chart 12: 7% of the survey base responded 'Don't know'.

International Concerns Persist

As mentioned earlier in the report, many merchants are looking to the international market as a strategy for growth. However, such aggressive expansion plans do not come without their concerns. Indeed, one in four merchants actually stopped accepting orders from certain countries outside the UK in 2009 due to high fraud levels (Chart 13). These merchants were asked which countries were no longer served – Nigeria stands out, with over 60% of respondents citing the country.

Countries No Longer Served Due to Fraud Levels

13



INDUSTRY
comment

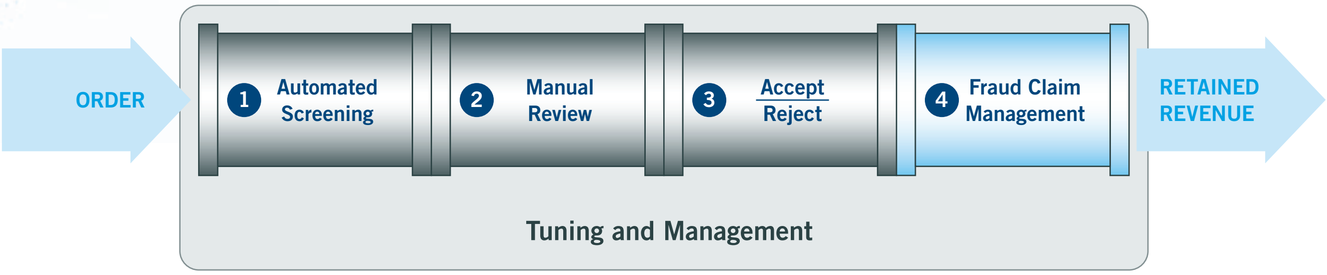
Compared to their predecessors, today's fraudsters are well organised, highly sophisticated and operate easily across international borders. This evolution is due in part to the ongoing implementation of preventative measures. Chip and PIN, for example, shifted the fraudsters' attention to transactions where the payment card was not present at the point of sale. Card not present transactions raise a completely different set of considerations to those that are traditionally conducted face-to-face with the consumer. For online, mail and telephone orders, effective fraud management rests on the ability of a merchant to confirm that the cardholder is legitimate.

Pre-empting the shift in fraud from face-to-face to card not present, Visa has been involved in developing technology to combat it. The continued uptake of 3D Secure authentication schemes, like Verified by Visa (VbV), is having an impact on fraudsters – making their 'jobs' that bit more difficult. Visa Europe has been working to optimise this service and experience with the planned introduction of an enhanced VbV user interface, bringing the customer experience of using VbV closely in line with the expectations of today's online consumers. This should be available for implementation by merchants during 2010. In order to preserve the integrity of the cardholder enrolment and authentication process within VbV, Visa is also promoting the move to dynamic authentication methods. One move in this direction is Visa CodeSure, a new type of card incorporating a keypad and LCD-screen, which is able to generate its own dynamic passcodes. This is currently being piloted by several banks in Europe.

Visa Europe is also working with its members to help them better understand the cost of fraud. By introducing the Total Cost of Fraud (TCoF) financial model, Visa Europe can further help member banks to better understand the wider business implications of their existing fraud management processes. Although designed for use by banks, the principles are equally relevant to merchants. As also described by CyberSource elsewhere in this report using their pipeline methodology, taking a wider view of the costs associated with fighting fraud can ensure that merchants and banks do not underestimate the associated costs, can reduce profit leaks, and increase the efficiency of their fraud management operations.

Kevin Smith
SVP Fraud Management, Visa Europe

Stage 4: Fraud Claim Management

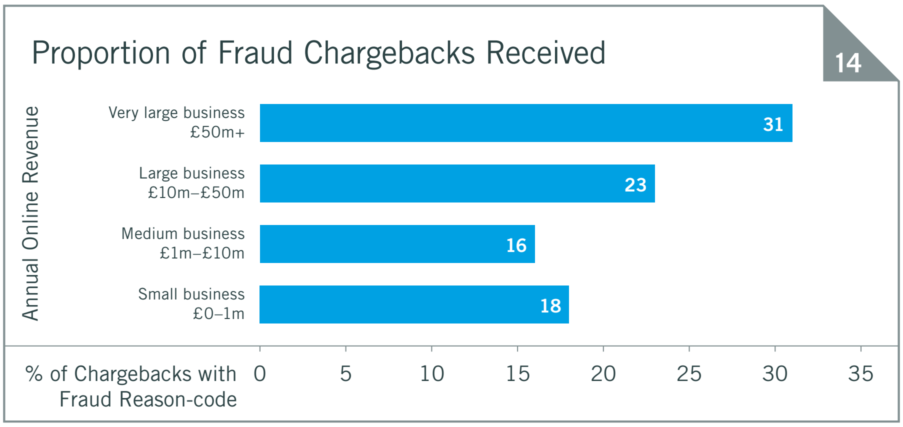


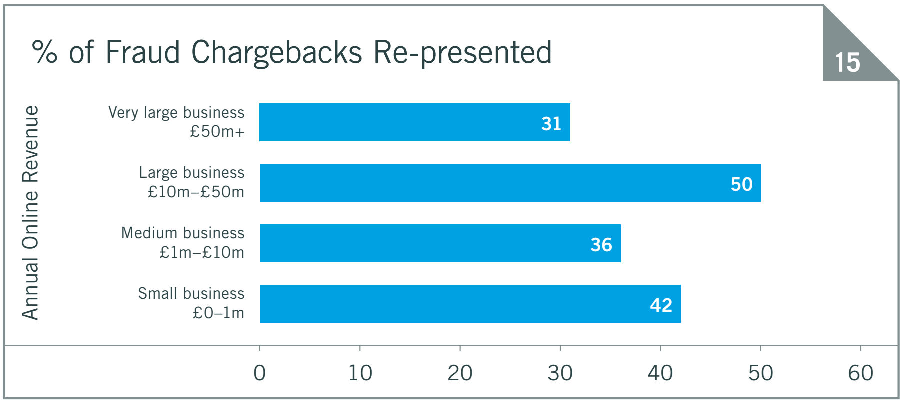
Fraud Chargebacks Have Significant Impact

The survey examined in more depth merchants' practices associated with the reviewing and contesting of chargebacks. Fraudulent orders are presented to the merchant via two main routes: as a direct request from a consumer for credit (they claim fraudulent use of their account) or as a chargeback. Of the chargebacks merchants receive, 23% (as a weighted average) are fraud reason-coded; this increases to 31% for very large businesses (Chart 14).

Considering the financial impact of both fraud claim routes (chargebacks and credit issuance/reversal) some organisations encourage direct consumer contact to address fraud claims and thus avoid the additional chargeback fees levied by the merchant bank/processor. Where a consumer contacts the merchant first, the merchant can either handle the dispute directly with the consumer or advise them to initiate a fraud chargeback process. If merchants are evaluating fraud losses solely on the basis of chargebacks, the actual rate of fraud loss experienced may be much higher because direct credit issuance will be absent from such reporting.

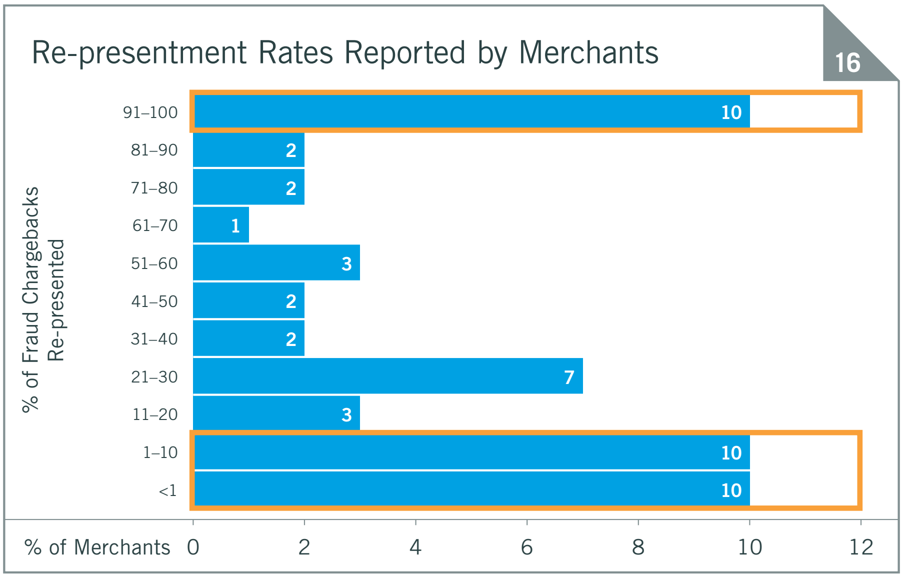
Of the fraud reason-coded chargebacks received, merchants re-present only 38%. Large businesses are most likely to contest fraud chargebacks, with 50% being re-presented (Chart 15)[4]. It should be noted that merchants using the 3D Secure schemes are typically shielded by their banks from individual chargeback claims, therefore a significant number are unable to see all of their fraud-coded chargebacks. That said, merchants should be looking to re-present chargebacks wherever possible – failure to do so may result in lost revenue.





[4] Chart 15: 23% of the survey base did not provide a response.

When looking at the distribution of re-presentment rates, it is evident that one in ten merchants is disputing more than 90% of their chargebacks (Chart 16). At the other end of the spectrum, one in ten is also re-presenting 1-10% of their chargebacks. The same proportion contests less than 1%. This bi-modal distribution is typical as it shows how merchants fall into three groups: the first, those that dispute everything; the second, those that dispute very little and the last, the broad group in the middle, that only dispute some chargebacks. Interestingly, this distribution has historically also been mirrored by the corresponding US online fraud surveys.



Win Rates Lower Than In North America

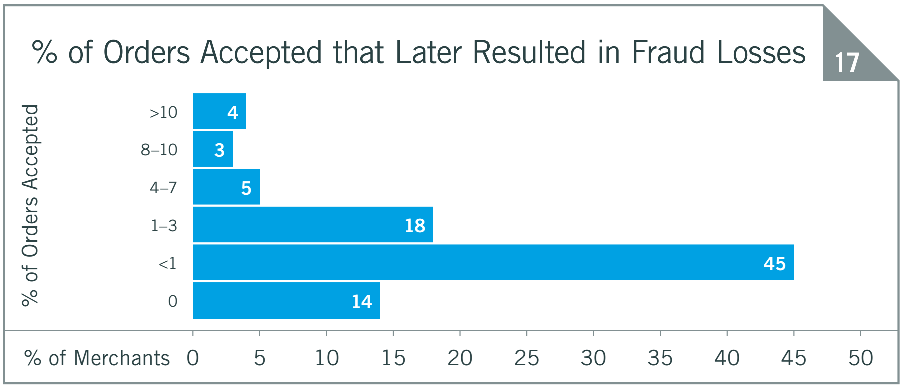
Merchants report that they win, on average, 34% of the chargebacks they dispute. In North America this number is slightly higher with merchants reporting a win-rate in the region of 40% over the last four years.

Disputing chargebacks is not an easy or cost-free process. Merchants must manage and organise all order, delivery and payment information to successfully dispute fraudulent orders with financial institutions. Ensuring that the right information is included in the correct amount of time will help businesses streamline the process and avoid unnecessary cost implications. Fraud chargeback management is a significant expense for merchants, but one that can be improved. With that in mind, a number of merchants are now looking to outsource this aspect of the pipeline to cut the time it takes to fight a chargeback and help improve the chance of winning their case.

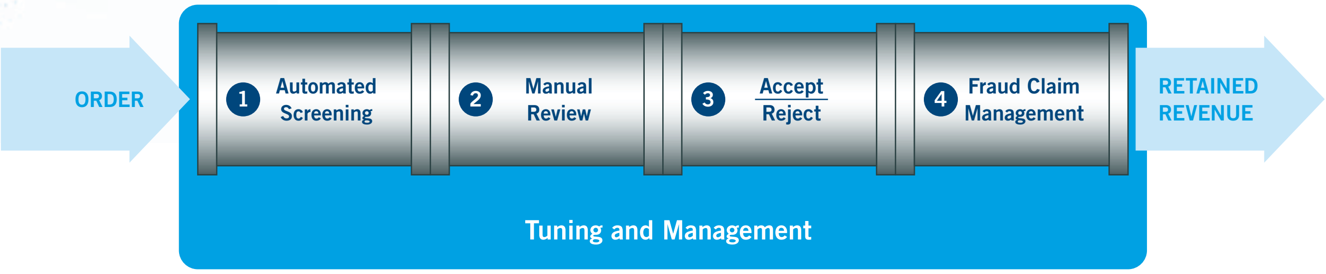
Fraudulent Order Rate Averages 1.6%

Another key metric is the percentage of accepted orders that later turn out to be fraudulent. It is typically lower than the revenue lost percentage. This is because the average value of fraudulent orders tends to be higher than that of valid orders, causing the fraud rate as measured by revenues to be higher. On average, 1.6% of accepted orders ultimately prove to be fraudulent.

In 2008, 8% of businesses experienced fraud on more than one in ten accepted orders. For 2009, only 4% of merchants saw this level of fraud (Chart 17). Overall, 30% of merchants reported a fraudulent order rate of 1% or more in 2009, representing a decrease of 11% on the previous year. Encouragingly, a higher volume of merchants (45%) reported that their fraudulent order rate was under 1%, compared to 2008.



Tuning & Management



Merchants Have More Complex Requirements

Having an automated order screening system in place with the appropriate interface allows business managers to modify decision rules without assistance from internal IT staff or external parties. The ability to adjust rules quickly helps to manage the order review flow, tailor rules to new products and adapt to new fraud trends as they are encountered. Without this ability, merchants cannot easily minimise reject rates, review costs or fraud rates. Additionally, giving business managers the capability to adjust business rules on-the-fly reduces the costs and burden of IT support.

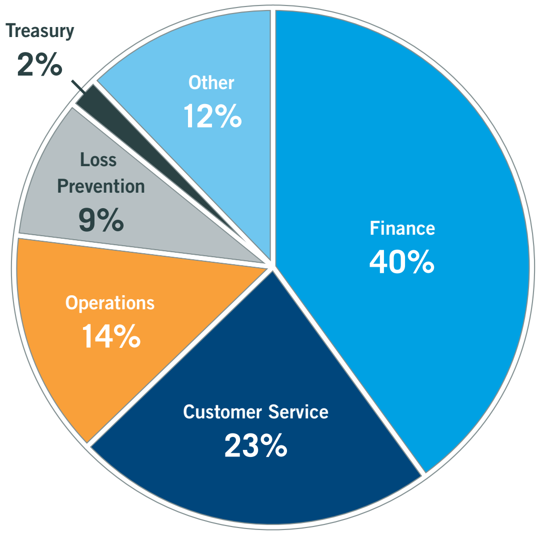
Some online merchants are integrating fraud tools and strategies via fraud management portals. These portals employ a combination of flexible rules systems that interact with a portfolio of 'truth services' around the globe, allowing business managers to set payment type, product type and market-specific screens. Case management systems are often integrated with these portals to streamline workflow. Global fraud portals typically include hierarchical management, as companies strive to centralise fraud management across multiple lines of business and geographies.

Fraud Management Responsibility Varies...

In the latest survey, we asked who has responsibility for the company's fraud management operation. For the majority of organisations (40%), it is the finance division that is responsible for the fraud team (Chart 18), although large companies are more likely to have a dedicated 'loss prevention' function. Interestingly, 23% of respondents cited their customer service departments as being responsible for their fraud teams. Ultimately, this ownership will depend on the structure of each organisation – there is certainly not one correct approach. In a number of businesses, fraud management responsibility may cut across multiple departments and even countries. In these instances, it is even more important to ensure that cross-function communication channels and policies are not only in place, but optimised.

Departments with Fraud Management Responsibility

18



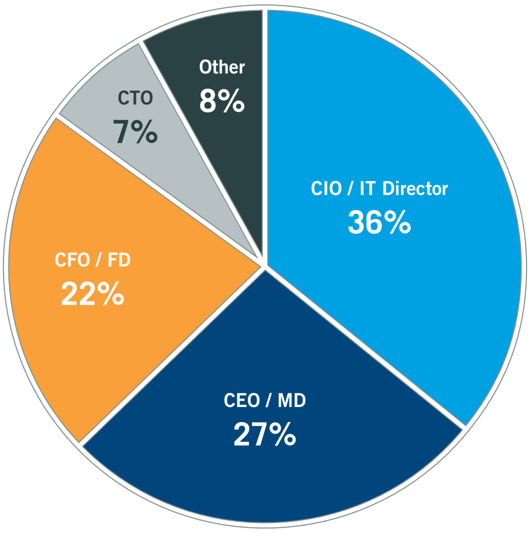
…As Does Payment Security Management

Data security and PCI compliance is another area where responsibility varies across organisations (Chart 19). CIOs/IT Directors tend to be held accountable in most organisations (36%), although the CEO/MD is not far behind (27%). The person responsible for the payment security policy should have complete visibility of their organisation's end-to-end approach to managing sensitive data. This is not simply about data storage, but moreover, all system and human interaction with payment data – this can make the task incredibly complex.

With eCommerce playing an increasingly important role in the new world order, merchants should ensure that their fraud and payment security strategies occupy a place within the highest echelons of their organisation. In doing so, strategies can be debated and defined at the most senior level, then disseminated throughout the business.

Responsibility for Data Security / PCI Compliance

19



INDUSTRY
comment

In the last CyberSource Online Fraud Report, I outlined the remit and goals of the recently created Police Central e-Crime Unit (PCeU). Over the past year, we have developed working partnerships at both a local and national level, in order to provide a more time critical response to cybercrime and capitalise on industry intelligence.

The creation of a UK hub to take action against cybercrime has been welcomed by a range of industry stakeholders, from police forces around the world, IT and financial communities, and service providers, to the public. There is general agreement that this is an effective mechanism through which to identify emerging cybercrime threats and provide the appropriate operational response.

Successes thus far include Operation Lumpfish, a joint initiative with US law enforcement, which revolved around fraudulent international online music sales, and Operation Phyllite. The latter culminated in the closure of more than 100 websites selling fake Premiership football tickets. The PCeU is planning to run a similar operation in the run-up to the 2012 Olympics, as we recognise that the Games could present a very real opportunity for large scale fraudulent activity.

Looking ahead, we see industry partnerships as critical to the success of the Unit. We will continue to cement partnerships with both industry and government agencies to help enhance national policing and disseminate advice on good practice and appropriate prevention techniques. We are also proposing that a further task force be established in relation to government and retail sectors; in doing so we can take a more holistic approach and ensure that we have the right people in place to provide a truly integrated intelligence picture, disrupting criminal networks and increasing prosecutions.

Detective Superintendent Charlie McMurdie
Police Central e-Crime Unit (PCeU)

Consumers & Online Fraud

Half of UK Consumers Don't Shop Online

For the third consecutive year, we have sought to better understand consumers' online shopping habits and fears. Data from 1004 adults, aged 16+, was collected during the weekend of the 16-18 October 2009. The survey group was designed to be nationally representative of adults throughout the United Kingdom, and weighting was applied to the results to bring the data in line with national profiles.

The results show that 50% of consumers still don't buy online, compared with 51% in 2008, and 54% in 2007. This represents a very large untapped market. Unsurprisingly, consumers aged 16-54 shopped over the internet more frequently than respondents aged 55+. In 2008, consumers from London showed the highest rate of eCommerce adoption, whereas in 2009 the rates were fairly similar across the whole of the UK. The same goes for gender; there is no material difference between males or females. The 2009 results also show that the rate at which consumers are adopting eCommerce would seem to be slowing, even in light of the growth in online retail.

Saving Time is a Key Motivator

We also asked consumers about their reasons for shopping online, or otherwise. For those respondents that do shop on the internet, their primary motivator is to save time and hassle (83%). Other significant reasons included immediate access to a wide range of products and services (73%) and greater cost savings (61%).

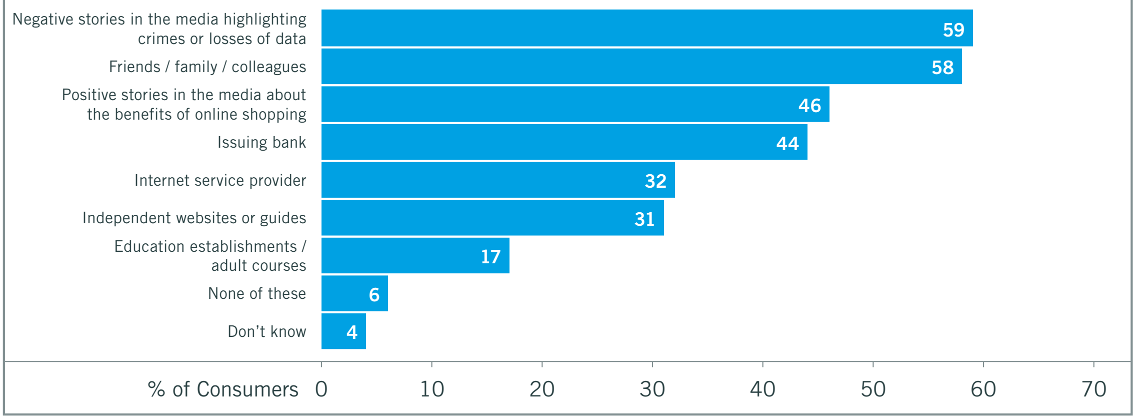
The majority of those that do not purchase online stated that they simply preferred buying on the high street (67%). With this in mind, a number of online retailers are identifying new ways of connecting with their existing and potential customer base. For instance, some are investing in the development of online communities to help create a sense of belonging. It is important to note that 41% of those who do not shop online stated they were concerned about the security of doing so – this is certainly an area that merchants, as well as the eCommerce industry as a whole, can seek to address.

Risk of Fraud Remains a Concern

Of the total sample of consumers surveyed, 71% are concerned with the level of risk when purchasing over the web, an increase of 5% on 2008. Consumers were asked where they hear information about the safety of shopping online – the majority cited the media. Respondents noted that they hear more negative stories (59%) than positive news (46%). The media can have a real impact on consumers, with news stories constantly filtering down – indeed, 58% of respondents stated that they receive information from their personal networks of friends, family and colleagues (Chart 20). On a separate note, just over a third of consumers have been a victim of online credit card fraud, or know someone that has. This is also undoubtedly impacting consumers' views about the safety of shopping on the web.

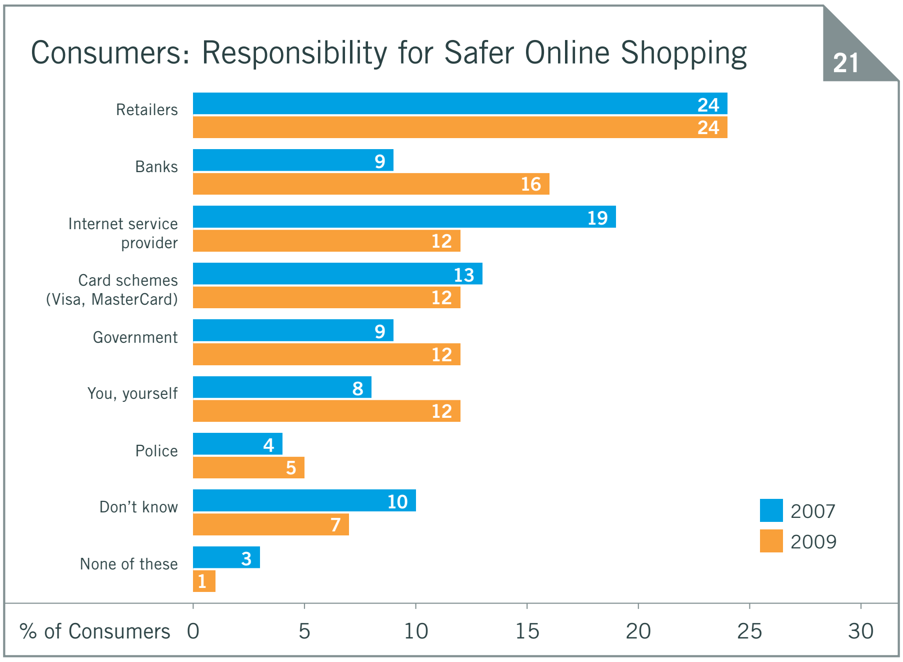
Consumers: Sources of Information About Online Safety

20



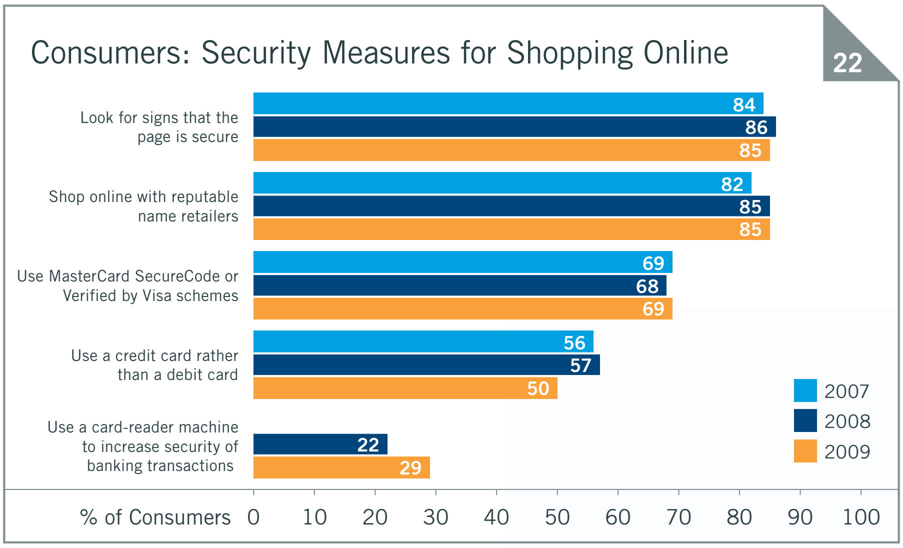
Retailers Responsible for Safer Online Shopping

We first asked consumers who should have responsibility for making online shopping safer in 2007. At this time, the results showed that 24% believed retailers were primarily responsible. In 2009, the response was exactly the same (Chart 21) – as far as consumers are concerned, nearly a quarter continue to hold merchants accountable. Other key trends are an increase in the accountability of banks in the eyes of consumers (16%), and a decline in the responsibility of internet service providers (12%). Furthermore, whilst the proportion of consumers accepting primary responsibility has increased since 2007, at 12% it is still just half the figure for retailers. The police are deemed to have only a marginal responsibility for making online shopping safer (5%).


Consumers: Responsibility for Safer Online Shopping

21

Over the years, there have been a few minor changes in the measures that consumers take to protect themselves when buying on the internet (Chart 22). The majority of respondents (85%) look for signs that the page is secure, such as the green address bar. Similarly, 85% of consumers surveyed ensure that they only buy online from reputable retailers. 3D Secure schemes are being employed by 69% of respondents, whilst card reader usage has increased slightly – in all, 29% of consumers now utilise such devices as part of their online banking process.


Consumers: Security Measures for Shopping Online

22

Uncertainty Surrounds Data Security

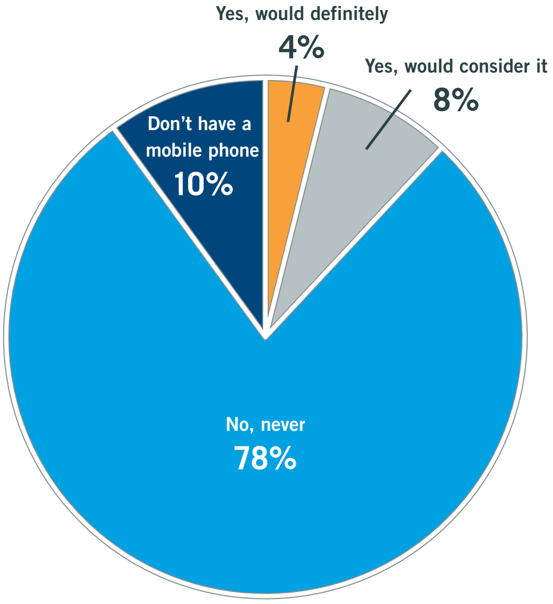
In the latest survey, we asked consumers for their feedback on data security. A significant proportion, 59%, reported that they were not comfortable with retailers storing their payment card data. This highlights the uncertainty that exists about data security, perhaps a result of the high profile breaches that have occurred during the past few years. Encouragingly, when looking purely at the consumers that shop online, 68% trust retailers with their personal details and payment information. In all, 65% of consumers buying over the internet felt they would be informed by the merchant, bank or internet service provider if their personal details were compromised. Businesses should ensure that they are effectively communicating their payment security policies, proactively reassuring customers and clearly displaying the measures they take to protect payment information.

The Mobile Opportunity?

Mobile payments have been touted as the ‘next big thing’ for some time now, but what do consumers actually think? The consumer survey revealed that, contrary to the mobile payments hype, 78% of all respondents said they would never use a mobile to make purchases online (Chart 23). Interestingly, when looking purely at consumers that buy on the internet, the results were very similar; 76% reported that they wouldn’t use a mobile in this manner. Mobile payments mean different things to different people; this undoubtedly contributes to a lack of consumer understanding of, and trust in, the concept. It will be interesting to see how the consumer response evolves in the coming years, as manufacturers introduce new devices capable of delivering a powerful user experience, and mobile payments become more mainstream.

Would You Use Your Mobile to Purchase Online?

23



One of the main challenges for merchants is that the term mobile payments is very general and covers multiple methods of customer interaction. Currently, if a customer uses a browser on their phone to view a standard website and place an order using a credit or debit card, this can be considered a mobile payment. At the other end of the spectrum, a merchant might work with a partner to offer an operator billing model. In this case, the consumer browses to a specific mobile-only site on their device and places an order. This purchase is added to their mobile phone bill as opposed to using a credit or debit card, and is also a type of mobile payment.

The level of risk that a merchant faces will clearly be different in each of these cases. Where the customer is entering card details into a browser on a mobile device, then many of the traditional checks the merchant uses will apply. However, it should be noted that analysis of the IP address location may prove to be misleading.

If the operator billing model is being used, traditional card fraud checks would not apply. The key aspect here is that merchants need to understand the end-to-end process they are deploying, and ensure they are aware where the liability lies for any fraud that is carried out. Mobile payments may be the next big thing, and fraudsters will certainly be looking to exploit this new channel, but until adoption increases it’s too early to tell exactly where the risk lies for merchants.

Conclusion

2009 was a testing year for many organisations, and whilst the online sales channel may have seen less impact than elsewhere, it did not emerge unscathed. Merchants have indicated that they are optimistic about 2010 and the vast majority expect to see growth in their online revenues. Significantly, this number is much higher than it was just 12 months prior. There is also a lot of enthusiasm about international expansion, an area that many online retailers are already embracing.

If merchants are to capitalise on the opportunity for online growth in uncertain times, it is more important than ever before that they optimise their payment and fraud management processes. Organisations are losing a considerable amount of revenue to online fraud across their risk pipelines, and this certainly needs to be addressed.

Overall, order rejection rates are not declining year-on-year and there is continued reliance on manual review. Merchants should look to reduce the need for review, whilst at the same time increasing both the efficiency and effectiveness of their reviewers. As eCommerce sales continue to grow, and some resources remain relatively fixed, merchants will face the challenge of screening more online orders, yet keeping rejection and fraud rates as low as possible.

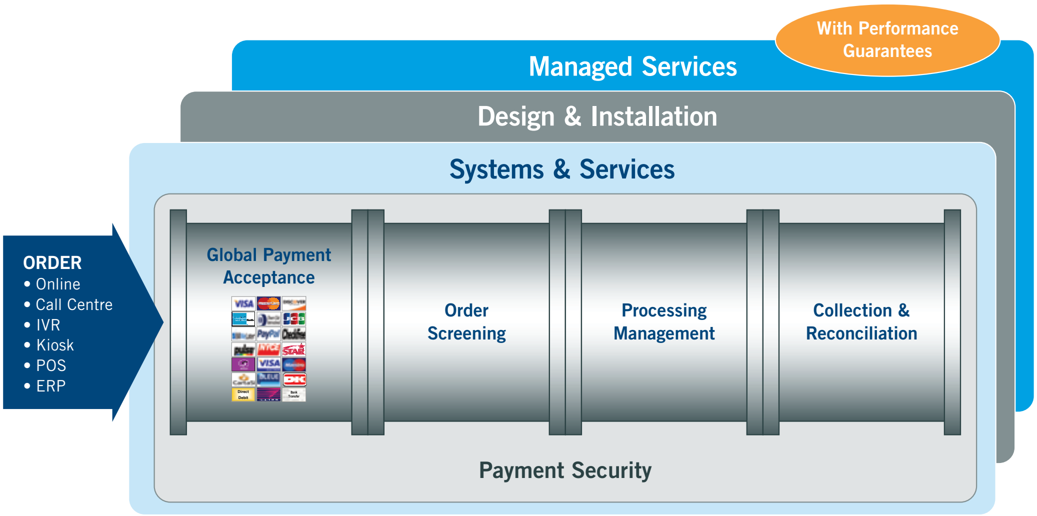
Significantly, consumers continue to view retailers as being primarily responsible for making online shopping safer. It is instead a collaborative effort, and one that requires continued investment from the many stakeholders, including government, police, banks, card schemes and payment vendors. Efforts would seem to be gathering pace however, with organisations like the PCeU reporting success across a number of anti-fraud operations. Stakeholders should ensure that they are working towards the same common set of goals, continuing to educate all on the benefits of online shopping, as well as the appropriate fraud and security measures that need to be adopted as standard.

Resources & Solutions

CyberSource is the world's first payment management company. We provide solutions that optimise business results and boost revenue through active management of the entire payment process – from global payment acceptance and processing, through to order screening, fraud management and enterprise payment security.

CyberSource Payment Management Solutions

CyberSource offers a comprehensive portfolio of modular services to help your company manage the entire payment pipeline. All are available via one connection to our web-based services.



Global Payment Acceptance

Accept multiple payment types using a merchant account from your preferred provider or CyberSource – including worldwide credit/debit cards, regional cards, direct debit, bank transfers and alternative payment types, such as PayPal. CyberSource also provides professional services to help you integrate payment with front-end and back-office systems.

We process your payments in our high availability datacentres located in the US, Europe and Japan. All datacentres are certified PCI-compliant and include sophisticated processing management logic to help prevent payment failures and rate downgrades.

A full array of online and exportable payment reporting capability is available to streamline reconciliation activity. Furthermore, systems can be installed to automate many of the tasks associated with payment reconciliation.

Fraud Management/Order Screening

Global Fraud Management Portal – A hosted rules and case management system provides on-demand access to over 200 validation tests and services across all four dimensions of detection. Detectors include: multi-merchant transaction history checks, worldwide delivery address and phone verification, device fingerprinting, IP geolocation, purchase velocity, identity morphing and custom data from your systems. A case management system provides consolidated data review and workflow management.

Managed Services – CyberSource provides client services to help you analyse, design and manage your order screening and fraud detection processes – everything from screening strategies and risk threshold optimisation analysis to ongoing monitoring and order review. Our managed services can include business performance guarantees.

How we can help your business

The CyberSource Managed Service team can add demonstrable value to your fraud screening processes. During 2009, our team helped a merchant in the travel sector reduce their automated order rejection rate by 80% and the number of orders being sent to manual review by 60%, whilst maintaining an acceptably low chargeback rate.

In another example, our experts worked with a high street retailer to increase their automated order acceptance rate by 20% whilst reducing their automated order rejection rate by 64%, again maintaining chargeback rates below agreed upon levels. These are prime examples of how, by focusing on more than just chargebacks, we can help to realise efficiency gains and cost savings for our customers.

Payer Authentication – Provides the online payment guarantees offered by Verified by Visa and MasterCard SecureCode.

Payment Security

Payment Tokenisation and Secure Storage – CyberSource provides payment tokenisation with remote secure storage and hosted payment acceptance services that let you capture and process payments without storing or transmitting payment data. This is a great way to streamline PCI compliance and mitigate security risk. Our outsourced screening management service can help you further eliminate staff contact with payment data.

Payment System Centralisation – Our team of experts will help you consolidate multiple payment systems into a single, easy to manage system. Optionally, CyberSource will also host, support and manage these systems in our secure datacentre.

Professional Services

CyberSource maintains a team of experienced payment consultants to assist with payment systems planning, system and process design, and implementation and integration. Our client services team is also available to help you monitor, tune, or fully outsource portions of your payment operations.

If you would like to receive more information about our solutions, please contact us on:-

Call +44 (0)118 929 4840

Email uk@cybersource.com

Visit www.cybersource.co.uk

About CyberSource

CyberSource is more than a global payment gateway or merchant services provider. We are focused on solutions that optimise business results and boost revenue through active management of the entire payment process – from global payment acceptance and processing, through to order screening, fraud management and enterprise payment security.

Founded in 1994, CyberSource pioneered online fraud screening at the inception of eCommerce. Today, through continued innovation and investment, we offer a comprehensive set of high performance payment management solutions for multiple sales channels, including the web and call centres. With a customer list that includes lastminute.com, British Airways and Nike, we enable our merchants to sell online in over 190 markets worldwide, helping them to protect, optimise and grow their operations.

Headquartered in the United States, we have operations across the world, including the United Kingdom, Singapore and Japan.

Global Offices

EMEA
CyberSource Ltd
The Waterfront
300 Thames Valley Park Drive
Reading RG6 1PT
UK
Phone: +44 (0)118 929 4840
Fax: +44 (0)118 929 4841
Email: uk@cybersource.com

Americas
CyberSource Corporation
1295 Charleston Road
Mountain View
CA 94043
USA
Phone: +1 650 965 6000
Fax: +1 650 625 9145
Email: sales@cybersource.com

Asia Pacific
CYBS Singapore Pte Ltd
Level 25, One Raffles Quay
Singapore, 048583
Phone: +65 6622 5623
Fax: +65 6622 5999
Email: asia@cybersource.com

CyberSource KK
3-11-11, IVY East Bldg 6F
Shibuya, Shibuya-ku
Tokyo 150-0002
Japan
Phone: +81 (0)3 5774 7733
Fax: +81 (0)3 5774 7732
Email: mail@cybersource.co.jp

www.cybersource.co.uk