Methodology

For the seventh 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 200 merchants and undertaken in-depth analysis of the results. Comparisons are drawn with previous reports, as well as the latest US fraud survey.

Included within this report is best practice advice for businesses trading online, together with industry comments from Visa and a Detective Superintendent from 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 an influence over, online fraud policy and decisions on the management of fraud. They revealed details about their revenues and expenditure, their operations, and more importantly, their experience with fraud and how they defend themselves. The analysis of these responses provides insight into how fraud is impacting the overall eCommerce industry.

The UK Online Fraud Report is designed to present an end-to-end view of the fraud management process – from automated screening and manual review, to order dispositioning and fraud claim management. The report also highlights merchant eCommerce expansion across international territories and provides guidance on how businesses can best protect themselves against the associated risks. Presented throughout is a selection of the key results from the survey, as well as the latest eCommerce industry trends and challenges merchants are facing.

Co-Authored by Dr Akif Khan, Director, Products and Services, CyberSource

As Director, Products and Services, at CyberSource, Dr Akif Khan is recognised as a progressive thought-leader in the eCommerce industry. Regularly in demand as a consultant and speaker within the online fraud arena, he assists and advises businesses globally. Dr Khan has witnessed first-hand the challenges faced by organisations in multiple geographies and market sectors.

Over the last year, Dr Khan has also helped to shape data security best practices, leading to the development of a framework that organisations can use to evolve their payment security policies and strategies.

As with previous reports, Dr Khan has been instrumental in consulting on the findings presented in this report, as well as offering counsel on payment optimisation trends and the future eCommerce landscape.
# Table of Contents

The Survey Base; Today's UK Online Business .......................... 02

Executive Summary .......................................................... 03

Setting the Scene ............................................................ 05

Stage 1: Automated Screening ............................................. 08

Stage 2: Manual Review .................................................... 11

Stage 3: Order Dispositioning (Accept/Reject) ....................... 15

Stage 4: Fraud Claim Management ...................................... 18

Tuning & Management ...................................................... 21

Conclusion ................................................................. 23

Resources & Solutions ..................................................... 24
To compile the UK Online Fraud Report, we asked merchants a series of questions about their business and the impact of online payment fraud. In terms of annual online revenue, there was a reasonably even split between merchant respondents classified as a medium business (£500,000–£5m), large business (£5m–£25m) and very large business (more than £25m). Small business respondents (less than £500,000) accounted for 15% of the survey base (Chart 1).

Respondents covered a diverse range of business sectors (Chart 2). In total, just over a third were retailers of physical goods (including clothing, books/DVDs, health and beauty and office supplies); 26% were selling services (including consumer finance, payment services, business services, advertising, education, government and charity); 21% were digital goods retailers (such as online news, publishing, online games, social networking and downloadable music/movies) and 17% were in the travel industry (such as hotels, car rental/rail/cruise, travel agencies and tour operators). This year respondents were more evenly distributed across sectors in comparison to the last survey, when over half were physical goods merchants.
Managing online fraud continues to be a significant and growing cost for merchants of all sizes. To better understand the impact of payment fraud on businesses selling over the internet, CyberSource sponsors annual surveys addressing the detection, prevention and management of online fraud. This report summarises findings from the seventh annual UK survey and is designed to help merchants make informed decisions about the most appropriate ways to protect their organisations.

Reshaping the Economic Landscape

In the previous survey, merchants forecasted a 68% increase in their 2009 online revenue, with 18% of merchants forecasting a fall; fairly encouraging feedback in light of the financial turmoil. In 2010, respondents appeared even more positive. At the time of the survey, three quarters estimated that their online revenues would grow in 2010, with only 2% expecting a decline. Such optimism was shared by businesses of all sizes, although very large organisations, with online revenues of more than £25m, appeared to be more confident; 83% anticipated an increase in 2010 compared to 59% of small businesses (with online revenues of less than £500,000).

Businesses estimate that their 2010 online revenues will have risen by an average of 34% year-on-year. More than two thirds of the respondents expecting growth predict an increase of up to 20%; within this group it is the small to medium sized businesses that are experiencing the highest growth rates.

Looking towards the future, on average, 77% of organisations are anticipating an increase in online revenues during 2011, whilst 21% believe that they will see no change (Chart 3). It is the medium and very large businesses that are demonstrating the greatest confidence; four in every five are expecting growth. Large organisations are just behind; their results are in line with the survey average. When examining the results by sector, travel merchants are most positive about online revenue growth (86% anticipate an increase).

For 2011, nearly four out of five merchants that are forecasting growth expect to see increases in eCommerce revenue of up to 40%. It is worth noting that historically, merchants have tended to underestimate their growth predictions for the year ahead. In times of continued economic uncertainty, this should provide even more comfort to organisations in 2011.
The Cost of Fraud

On average, the percentage of annual online revenue that businesses expect to lose to payment fraud in 2010 has dropped from 1.8% to 1.6%. The survey revealed that this does vary dramatically by merchant size: very large businesses expected to lose 1.5% to online payment fraud, equating to an average of £365,500; large businesses expect to lose £173,500 (1.2%); medium businesses £66,000 (2.4%); small businesses £3,500 (1.5%). Significantly, 39% of merchants expect to lose less than 1% of revenue to online fraud in 2010.

For 2011, over a third of businesses are expecting to see the percentage of web revenue lost to fraud grow year-on-year – a slight increase since the last report. However, 64% of merchants do not expect the figure to grow, which is encouraging.

Changing Business Threats

As with previous years, we asked merchants to rank the greatest threats to their business in an effort to identify the key challenges and advise on the best ways to address them. Online fraud continues to be rated as the greatest business threat (59%) – there has been a very gradual increase over the years, and the threat is certainly not deemed to be abating (Chart 4). Interestingly, more digital goods companies ranked online fraud as the most serious threat (72%) than respondents from other sectors.

Systems failure has overtaken the theft of customer data as one of the top two concerns for merchants. They have grown increasingly aware of the impact that both internal and external failures can have upon their business – particularly when a large proportion of the revenue stream is derived from online sales channels.

Manual Review Burden

Overall, 64% of the merchants surveyed use manual review; this has declined slightly from the 70% reported in 2009. However, the proportion of businesses reviewing every order has risen to 9%. The average number of manual review team heads has grown significantly, despite the majority of merchants predicting in 2009 that team sizes would not increase in the following year. This does vary by business sector.

As part of the survey, we asked merchants about their key fraud management focus areas for 2011. The cost of manual review has become a big concern for companies; not surprisingly, 29% stated that their main priority in the next 12 months is to improve automated detection and sorting capabilities, in an effort to reduce the number of orders being sent for review.

Businesses are also looking to improve process analytics (31%) and streamline task and workflow management during the manual review process (17%). Significantly, just over a third of small companies do not know what their future priorities for business process improvement are.
Setting the Scene

The UK Online Fraud Report series has provided an in-depth view of the ways in which merchants evolve their online fraud management processes in response to changing customer demands, the expansion of eCommerce channels and the increasing sophistication of fraudsters. Businesses are under pressure to offer consumers the widest range of relevant payment options, whilst implementing new fraud tools and techniques that keep the business, as well as their customers, safe.

Plastic Cards Dominate

Credit and debit cards continue to be the most popular form of payment acceptance, with 94% of merchants surveyed accepting them. A few payment types have seen a rise in acceptance levels; for instance, 41% of merchants now offer PayPal compared to 32% in the last survey.

UK merchants are increasingly accepting payment in currencies other than GBP (27%); furthermore 15% of respondents accept cards specific to regions outside the UK, such as Carte Bleue. Other forms of payment have plateaued, such as bank transfer and direct debit, at 31% and 27% respectively. The adoption of Google Checkout has only risen by 1% since the previous survey to 10%, whilst mobile payments acceptance is only reported to have grown to 5%.

Whilst the mobile channel will most certainly increase in significance for online retailers, it is still too early to understand what the dominant operating model will be. Some retailers are focused on creating versions of their websites that are optimised for display on mobile phones; others are ditching the browser and adopting the ‘app’ approach. Depending on the cost of goods being sold, some merchants are taking card payments via the mobile device (by means of a browser or app) whilst others are adopting the operator billing model, whereby items are charged to the consumer’s mobile phone bill. The other key consideration is fraud; again it’s too early to tell how fraudsters will attempt to exploit this nascent channel, and in turn how retailers will be able to defend themselves.

International Expansion Continues

Expansion into other territories is an area that UK merchants have been embracing for some time, with many already selling into Europe, the Americas and Asia Pacific (APAC). In total, 59% of respondents stated that they are accepting online orders from overseas (meaning that when fulfilled, the order is shipped to or downloaded in a country outside the UK). Not surprisingly, digital goods merchants report a much higher percentage of international web orders; an average of 35%, compared to physical goods retailers at 17%.

In this report we have observed increases in acceptance across all countries identified in the associated survey; in some instances this growth has been quite dramatic, particularly in the APAC region. Japan is now well served by UK merchants that sell internationally (up to 43%, compared to 25% in the previous survey), as are Australia, Hong Kong, Singapore and China.

Within the Americas, the USA and Canada have become increasingly important regions with 62% and 53% of merchants accepting orders from these countries respectively. Mexico and Brazil continue to grow but at a slower pace, with around a third of companies selling to these countries.

The majority of merchants surveyed accept orders from mainland Europe. In fact, France, Germany, Italy, the Netherlands and Spain are each served by over two thirds of the companies selling overseas, and Sweden is not far behind (Chart 5).

Future expansion for a number of regions is anticipated to slow in 2011; this is to be expected given the existing high penetration levels. When looking at the countries that merchants plan to add in 2011, the USA, Hong Kong, the Netherlands, Sweden and Italy top the list.
End-to-End 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. Alongside direct revenue costs, the cost of stolen goods/services and associated delivery/fulfilment costs, there are the additional costs such as: rejecting valid orders; staffing manual review teams; the administration of fraud claims; paying for the maintenance of internal systems; the cost of using third party tools. In addition, there are challenges associated with business scalability. Merchants can gain efficiency by taking a total pipeline view of operations and costs. Whilst the fraud rate is one metric to monitor, an end-to-end view is required to arrive at the best possible financial outcome.

A fraud management pipeline is used to illustrate some of the profit leaks that take place throughout the payment process. Over a third of businesses report that the percentage of online revenue lost to payment fraud has increased year-on-year. When we drill down into the detail, we find that merchants are rejecting on average 5% of incoming orders due to suspicion of fraud – this has increased from 4.6% in the last survey. More specifically, nearly a quarter of merchants reject more than 5% of orders, representing a high proportion of potential lost revenue. Interestingly, digital goods retailers reject the highest average number of orders (6.1%) due to suspicion of fraud.

Of the total number of orders merchants receive, one fifth are manually reviewed for potential online payment fraud, a slight increase since the last survey. Yet, of the orders reviewed, 71% are ultimately accepted. Overall, 1.9% of accepted orders result in fraud losses, an increase from 1.6% in 2009. It is important to note that this figure does vary by size and type of business.

The 2011 UK Online Fraud Report details key metrics and practices at each point in the fraud management pipeline in order to provide benchmarks and additional insight for businesses trading online.

Fraud Management Pipeline

![Fraud Management Pipeline Diagram](image)
Reviewing Automated Screening

Automated detection tools are used to identify the probability of risk associated with a transaction, or to validate the identity of the purchaser. The subsequent results of these tests are then interpreted by reviewers or rules systems to determine if a transaction should be accepted, rejected or marked for further review. A wide variety of tools is available to help merchants evaluate incoming orders for potential fraud.

Those businesses that handle larger volumes of online orders tend to implement an automated order evaluation system, either internally or from a vendor, to assess whether an incoming order might carry a fraud risk. Some merchants will allow this automated screen to reject orders without further intervention. Significantly, only 3% of survey respondents claimed that they were not using any form of automated fraud detection.

Adopting a Multi-Layered Approach

3D Secure schemes (also known as payer authentication) such as Verified by Visa and MasterCard SecureCode continue to grow in popularity year-on-year (Chart 6), as predicted in the previous report. These password protected identity verification services provide an additional layer of security for merchants, helping to mitigate the risk of online fraud. By 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. Payer authentication will not be completely effective if used in isolation but when combined with other fraud screening tools, it can help merchants minimise the cost of fraud to their organisation.

Whilst still prevalent, digital goods retailers are less likely to use CVN (71%, compared to 81% of physical goods retailers and 88% of travel organisations) and payer authentication, in particular MasterCard SecureCode (60%, versus 79% of travel merchants). However, they are more likely than other sectors to use device fingerprinting – 12% compared to an average of 5% across other sectors. Device fingerprinting 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 compromised set of devices.
## Automated Fraud Detection Tool Current Usage and Plans

<table>
<thead>
<tr>
<th>Validation Services</th>
<th>Total %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verified by Visa</td>
<td>73</td>
</tr>
<tr>
<td>Card Verification Number</td>
<td>78</td>
</tr>
<tr>
<td>MasterCard SecureCode</td>
<td>67</td>
</tr>
<tr>
<td>Address Verification Service</td>
<td>61</td>
</tr>
<tr>
<td>Postal address validation services</td>
<td>38</td>
</tr>
<tr>
<td>Credit history checks</td>
<td>17</td>
</tr>
<tr>
<td>Paid-for public records services</td>
<td>15</td>
</tr>
<tr>
<td>Telephone number verification</td>
<td>13</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Single Merchant Purchase History</th>
<th>Total %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud scoring models – internal</td>
<td>40</td>
</tr>
<tr>
<td>Customer order history</td>
<td>38</td>
</tr>
<tr>
<td>Negative lists – in-house</td>
<td>29</td>
</tr>
<tr>
<td>Positive lists</td>
<td>22</td>
</tr>
<tr>
<td>Customer website behaviour/ pattern analysis</td>
<td>18</td>
</tr>
<tr>
<td>Order velocity monitoring</td>
<td>16</td>
</tr>
<tr>
<td>Purchase Device Tracing</td>
<td>19</td>
</tr>
<tr>
<td>IP geolocation</td>
<td>19</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Multi-Merchant Purchase History</th>
<th>Planning to implement in 2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared negative lists – hotlists</td>
<td>17</td>
</tr>
<tr>
<td>Purchase velocity/ identity morphing models</td>
<td>9</td>
</tr>
</tbody>
</table>

### Automated Screening Investment Planned

Merchants typically deploy a combination of six different automated anti-fraud tools; this has not changed since the previous survey. For very large organisations, seven tools is the standard, whilst small businesses typically deploy four tools as part of their automated screening process.

Merchants plan to continue investing in automated screening tools over the next 12 months. On average, 16% are looking to implement shared negative lists in 2011, 15% order velocity monitoring and 14% customer website behaviour/pattern analysis.

The investment objectives for 2011 vary depending on size of company. Very large businesses prioritise customer website behaviour/pattern analysis (19%) while smaller organisations plan to add positive lists and order velocity monitoring (both 14%).
Payment Security Concerns Remain

Payment security continues to be a priority for merchants. Over a third of respondents ranked the theft of customer data as their most serious business threat. When asked for more detail, 57% stated this was due to the costs and resources required to securely store and encrypt card data in-house being higher than anticipated. In total, 39% reported that their concerns were driven by the confusion that exists around PCI compliance and data security requirements (Chart 7).

When dealing with sensitive payment information, merchants can choose to store and process the data in-house (i.e. on-premises), outsource this responsibility to a third party (i.e. utilise a hosted model) or use a hybrid model which combines elements of both strategies. By managing the payment data in-house, merchants take on full responsibility for ensuring the information is stored securely and in compliance with PCI DSS standards. Merchants need to carefully consider which approach is right for their business.

Greatest Business Threats: Theft of Customer Data

<table>
<thead>
<tr>
<th>Threat</th>
<th>% of Merchants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Costs and resources required to securely store and encrypt card data</td>
<td>57%</td>
</tr>
<tr>
<td>in-house are higher than anticipated</td>
<td></td>
</tr>
<tr>
<td>Confusion around PCI compliance and data security requirements</td>
<td>39%</td>
</tr>
<tr>
<td>PCI compliance projects are not prioritised at a senior level within</td>
<td>29%</td>
</tr>
<tr>
<td>the business</td>
<td></td>
</tr>
<tr>
<td>Our current data security measures are inadequate to meet the perceived</td>
<td>21%</td>
</tr>
<tr>
<td>threat</td>
<td></td>
</tr>
</tbody>
</table>

Addressing Payment Security

Today’s merchants are increasingly concerned about the costs of managing data in-house, and are looking to determine the most appropriate strategy for their business (be it on-premises, hosted or a combination of both). We’ve designed a framework to help organisations more effectively identify the costs associated with the various models.

Long Transaction Lifecycle

Businesses operating across multiple channels and geographies have to deal with an ever more complex lifecycle. Transactions touch many different systems, departments and people; it is therefore vital that you know exactly who, and what, is touching sensitive data.

You should also understand all costs and risks associated with securing the transaction, including data capture and transmission, its storage and back office exposure. Many organisations focus their payment security efforts on the storage element, and overlook other areas.

Comprehensive Review of Costs

It’s important that you take a holistic view, particularly given the multiple costs associated with running a payment security programme.

1. **Personnel** – Review the number and roles of staff, as well as training requirements.

2. **Technology** – Consider the costs of the hardware, software and support required to maintain your programme. You should also bear in mind the costs of updating and upgrading systems; this is frequently overlooked.

3. **PCI DSS validation** – Incorporate the costs of annual certification, QSAs, audit logs and vulnerability scans.

Finally, ensure that you take a longer-term view when evaluating payment security costs and options. We recommend that you consider the next five years, as this will cover both the implementation and ongoing costs.
Stage 2: Manual Review

Order Review Rates Still High
Orders that are not accepted or rejected enter into a manual review queue. During this stage additional information may be collected to help determine if the order should be accepted; or rejected due to excessive fraud risk.

In all, 64% of merchants stated that they use manual review as part of their online fraud screening process, representing a small decrease since the last survey. Importantly, this figure is sector-specific and is much higher for physical goods retailers (77%) and travel organisations (70%). On the other hand, only 55% of digital goods merchants conduct manual reviews; this may be due to the more immediate fulfilment that is required for such orders.

Looking at the results by size of merchant, around three quarters of very large businesses are likely to employ manual review, compared to just 45% of small companies. This latter group is also less likely to have a dedicated review team, which might account for the differences in application. On average, one in five orders is subject to manual review and, although this also depends on merchant size. The smallest companies reported that they review over a third of transactions, whilst very large businesses have the lowest review rates at 13%; this is not surprising given their higher order volumes, as well as the fact that manual review is not easy to scale.

Significantly, 9% of respondents review almost every order, however this average is impacted by smaller merchants (23%) and medium businesses (14%) that are more likely to analyse each transaction. Aside from lower order volumes, they may not have implemented the sophisticated automated tools that are being used by larger organisations.

Multiple Tools Are Used
Many of the tools or detector results used during automated screening can also form part of the manual review process. That said, several additional tools and processes are utilised by reviewers for orders that require human interaction. Attempting to contact the customer to validate an order continues to be the most popular method employed to review orders; today it is standard practice for 71% of merchants, compared to almost 60% in the last survey (Chart 8).

Four in five very large organisations contact the customer, although the use of this method decreases by business size. Importantly, many companies 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. As per the last survey, the second most popular method is reviewing past customer order history; its application has grown from 50% to 61%.

The use of postal address validation services is now the third most popular tool, having increased by 10% since the last survey to 57%. Respondents report that their review teams typically employ an average of three tools, a decrease from four in 2009. Not surprisingly, small businesses tend to use just two tools; this is in contrast to very large businesses that utilise around four tools during the review stage.

Over the next 12 months, 11% of organisations will be considering outsourcing portions of their review and order screening operations. Manual review represents a critical area of profit leakage and if not managed effectively, it can be expensive, limit scalability and impact customer satisfaction.
Room For Greater Efficiency

The average size of manual review teams has risen quite considerably from an average of six full time staff members in 2009 to ten in 2010. Interestingly, it is one particular sector – services – that has accounted for this increase. When looking at the responses from organisations within the physical goods, digital goods and travel sectors, the average is closer to six.

In terms of manual review staffing plans for 2011, on average only 13% of merchants are planning to increase the size of their teams, and three quarters expect to make no changes (Chart 9). With 77% of merchants expecting to grow online revenues in 2011, it is absolutely vital that companies maximise the efficiency and effectiveness of existing staff. Firstly, the accuracy of automated sorting should receive greater attention in an effort to decrease the need for review. In addition, merchants should focus on how best to streamline the review process itself.

The survey found that each manual reviewer analyses an average of 77 orders per day. At very large businesses the number is even higher; nearly a quarter indicated that each reviewer checks more than 120 a day. In general it is the digital merchant teams that review the highest number of transactions per day.
Case Management More Popular

Of the merchants identifying online fraud as their most serious business threat, 56% were concerned that they are spending too much by reviewing too many orders. This compares to 44% of respondents that are concerned about the overall amount of revenue being lost to fraud (Chart 10). Attention is certainly being focused on the need to automate as much of the screening process as possible, as well as the need to streamline current review processes.

The survey found that 37% of merchants use a case management system to support their manual review process (Chart 11), an increase from 23% in the last survey. Case management systems consolidate order information and present the results for reviewers to assess and action as required. Not surprisingly, adoption is much higher within very large organisations, where nearly half of those surveyed employ such systems.

The use of case management systems is set to rise, with 29% of merchants anticipating their implementation over the next 12 months. This could potentially result in two thirds of merchants having a system in place to support their manual review process and staff by the end of 2011.
Case Management Usage

All Merchants

- Currently use: 37%
- Plan to implement in 2011: 29%
- Do not use or plan to implement: 34%

Merchants £25m+ Online Revenue

- Currently use: 48%
- Plan to implement in 2011: 28%
- Do not use or plan to implement: 24%

BEST PRACTICE advice

Optimising Manual Review

There are several things that merchants can do to improve the efficiency of their manual review processes. Firstly, using a case management system to consolidate all information relating to an order (customer details, previous orders, fraud screening results etc.) will prevent your reviewers having to switch between systems and spend time looking for data. Our experience has shown that large merchants that deploy such systems (either their own or from a vendor) have more productive review teams.

Secondly, it is vital to train your reviewers properly. Although some decisions may be based on ‘gut feel’, the majority should be undertaken within a structured framework, and include a series of documented checks that must be performed on each order.

Finally, use a system that enables you to gather accurate metrics on the performance of a review team. Statistics such as the time an order is in a queue before it is picked up, and the average time each reviewer spends per order, are all vital for you to gauge the health of the process, and to serve as a foundation for improvement.
Manual Review Inefficiencies Remain
Automated screening and manual review ultimately result in order acceptance or rejection. Merchants reported that a high percentage of manually reviewed orders are actually accepted – on average, 71% (Chart 12). This is similar across all sectors apart from one, digital goods – merchants in this sector noted that they only accept just over half of the orders sent for review (furthermore, as previously referenced, the use of manual review is less prevalent amongst digital goods merchants). Significantly, it is the small businesses that accept the highest percentage of reviewed orders, at 81%.

High Order Rejection Rates Persist
Order reject rates can be an important indicator of true fraud risk or signal profit leaks in terms of valid order rejection or high rates of manual review. The survey found that merchants reject, on average, 5% of orders due to suspicion of fraud. This figure has increased from 4.6% in the last survey. For the last few years this figure has remained relatively consistent; the fact that it is not decreasing should certainly cause merchants concern. It should however be noted that nearly 60% of businesses reject under 3% of orders due to fraud concerns (Chart 13).

Merchants should also bear in mind that not all the rejected orders will be fraudulent, representing lost revenue opportunities. Poor fraud screening, over-cautiousness and lack of expertise could all be contributing to high rejection rates. Whether merchants can decrease their overall order rejection rates without an increase in fraud rates or manual review remains to be seen.
Countries No Longer Served Due to Fraud Levels

**Asia Pacific**

<table>
<thead>
<tr>
<th>Country</th>
<th>2009</th>
<th>2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Singapore</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>Australia</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>India</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Japan</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>Indonesia</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>China</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td>Malaysia</td>
<td>10</td>
<td>8</td>
</tr>
<tr>
<td>Pakistan</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>South Korea</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>Taiwan</td>
<td>12</td>
<td>15</td>
</tr>
<tr>
<td>Philippines</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>Vietnam</td>
<td>15</td>
<td></td>
</tr>
</tbody>
</table>

**Europe, Middle East & Africa**

<table>
<thead>
<tr>
<th>Country</th>
<th>2009</th>
<th>2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>France</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Spain</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Italy</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>Germany</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>Romania</td>
<td>17</td>
<td>17</td>
</tr>
<tr>
<td>Russia</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td>Ghana</td>
<td>34</td>
<td>55</td>
</tr>
<tr>
<td>Nigeria</td>
<td>62</td>
<td></td>
</tr>
</tbody>
</table>

**Americas**

<table>
<thead>
<tr>
<th>Country</th>
<th>2009</th>
<th>2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brazil</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>Mexico</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>Canada</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>USA</td>
<td>25</td>
<td></td>
</tr>
</tbody>
</table>

2009 and 2010 percentages of merchants.
Concerns About International Expansion

The international expansion witnessed by many online retailers provides new revenue and growth opportunities, but with this comes the potential for new risks. Indeed, just over one in four merchants stopped accepting orders from certain countries outside the UK in 2010; this represents the same rate as 2009 (Chart 14).

Nigeria remains most frequently cited as the country no longer served by merchants (55%) — a response that is consistent across all verticals and sizes. This is followed by Ghana, which has been blacklisted by 34% of businesses, then, perhaps somewhat surprisingly, the USA (25%). The USA has become an increasingly popular market for merchants in recent years as they look to capitalise on a similar language and online buying culture. It may be that some merchants have looked to rapidly add new countries to their portfolios without the required due diligence.

In the latest survey we drilled deeper and asked merchants to provide feedback on the order identifiers they use when considering a country to be high risk. A total of 59% of merchants stated that they use the delivery address and 58%, IP address. Digital goods businesses are much more reliant on the IP address than the other sectors with three quarters using this identifier. Merchants should exercise caution if relying overly on the IP address, particularly given the increase in ‘cleaner fraud’.

A number of organisations are also using the billing address as an identifier for risky countries (55%). This should not be used in isolation because today’s fraudsters are better able to imitate legitimate transactions; characteristics like billing address can appear to be valid unless deeper analysis takes place. Although less popular, by using BIN information, merchants can cross reference against the customer’s bank records and check for further anomalies (Chart 15).

### High Risk Country Identifiers

<table>
<thead>
<tr>
<th>Identifier</th>
<th>% of Merchants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delivery address</td>
<td>59</td>
</tr>
<tr>
<td>IP address</td>
<td>58</td>
</tr>
<tr>
<td>Billing address</td>
<td>55</td>
</tr>
<tr>
<td>BIN country</td>
<td>25</td>
</tr>
<tr>
<td>Website on which the order was placed</td>
<td>16</td>
</tr>
</tbody>
</table>

The Rise in Cleaner Fraud

A significant trend that we’ve observed in the last year is an increase in what is termed cleaner fraud — meaning fraudulent transactions that look like good transactions. This reflects the growing sophistication of some fraudsters, who can place fraudulent orders with frustratingly consistent attributes (address, IP geolocation, card issuing country, phone number, etc.).

As a merchant, you will need to adopt the latest tools to identify some of these transactions as fraudulent. Device fingerprinting is the obvious choice, enabling you to see if seemingly unrelated transactions have in fact all originated from the same laptop, PC or mobile device. However, it’s important that you select vendors carefully. The more advanced options offer functionality that enables businesses to ‘pierce’ through proxies, which can be used by fraudsters to mask their true IP addresses.

To explain, a fraudster may be sitting in, say, Russia, but sending transactions via a proxy in, for example, the UK. An organisation using traditional IP geolocation checks will simply see that the ‘customer’ is in the UK — hence the transaction may look clean. By deploying the latest proxy piercing technology, you stand an increased chance of seeing that a proxy is being used and that the data is coming from Russia. This is the kind of insight required to defend your organisation from cleaner fraud.
Increase in Fraud Chargebacks

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 where they claim fraudulent use of their account, or as a chargeback.

On average, one third of the chargebacks merchants receive are fraud-coded. This figure does vary substantially depending on the merchant sector; travel organisations reported the highest number (48%) and digital goods the lowest (26%). Merchant size also has an impact; 52% of the chargebacks that large businesses receive are fraud-coded (Chart 16). It is much lower for other organisations.

The financial implications of both fraud claim routes (chargebacks and credit issuance/reversal) can be high, and subsequently, some organisations encourage direct consumer contact to address fraud claims, thus avoiding 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 organisations 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-coded chargebacks received, merchants re-present on average only 31%; a slight decrease since the last survey (38%). Very large businesses are more likely to contest fraud chargebacks, with 44% reporting this scenario (Chart 17). Travel merchants are also more likely to re-present (43%) compared to companies selling physical goods (33%), services (28%) and digital goods (24%).

It’s important to note that merchants using the 3D Secure schemes are typically shielded by their banks from individual chargeback claims. Therefore many businesses are unable to see all of their fraud-coded chargebacks. However, where possible, merchants should be looking to re-present chargebacks as failure to do so can result in lost revenue.

When looking at the distribution of re-presentation rates, it is apparent that 14% of merchants are disputing over 90% of their fraud-coded chargebacks (Chart 18). At the other end of the spectrum, nearly a third of businesses are contesting less than 1%. This distribution is fairly typical as merchants tend to fall into three groups: those that dispute everything; those that dispute very little; and the broad group in the middle that only dispute some.

Interestingly, both this survey and the last one show a peak for merchants disputing 20–30% of their fraud chargebacks; one in five merchants now reports this level.

Merchants report that they win, on average, 26% of the fraud-coded chargebacks that are re-presented. This success rate does vary by sector, with digital goods merchants stating that they win 34% of disputed fraud chargebacks.
Fraudulent Order Rates Relatively High

Another key metric that merchants can use when determining the effectiveness of fraud claim management is the percentage of accepted orders that later turn out to be fraudulent. On average, 1.9% of accepted orders ultimately prove to be fraudulent; this represents an increase from the 1.6% reported in the last survey. This figure has risen in 2010 due to the higher fraudulent order rates witnessed by digital goods merchants. However other sectors reported lower percentages; for example physical goods retailers have an average rate of 1.7%.

Digital goods merchants have a higher fraudulent order rate because fraud may have less impact on their business than a traditional physical goods retailer. Firstly, digital goods companies can make far higher margins on their products than physical goods retailers, so might be a little less cautious about releasing goods since losses can be made up by other sales. Secondly, if a digital goods merchant does sell an item (software application, ringtone, game, music etc.) and it turns out to be a fraud loss, it may not impact their stock or inventory – the business hasn’t lost a material item that needs to be replaced. As a result, they may err less on the side of caution than traditional physical goods retailers. This does not imply that digital goods merchants are complacent about fraud; they still need to meet the same standards of maintaining low fraud rates as dictated by the banks and card schemes.

In 2010, 8% of all respondents experienced fraud on more than one in 20 accepted orders (Chart 19). Overall, the number of merchants reporting fraudulent order rates of less than 1% has declined since 2009 (32% versus 45%), although this is offset by an increase in the number of businesses experiencing fraud on 1–3% of orders (39% versus 18% in 2009).

![Percentage of Fraudulent Orders by Industry](chart19.png)

Although there has been industry progress regarding online fraud, we should not be complacent that our task is done. As highlighted in this report, merchants must continue to adopt appropriate fraud prevention measures.

Verified by Visa (VbV) continues to be the primary merchant-facing fraud prevention measure advocated by Visa Europe. VbV penetration in the UK is now over 53% of all Visa card eCommerce transactions (as of September 2010), up from 47% for the same period last year. Over 90% of all UK VbV transactions are now fully authenticated (eci5). The UK performance contributes to corresponding Visa Europe-wide fraud reporting, which indicates that eCommerce transactions that are not fully authenticated are three times more likely to be disputed to merchants for fraud reasons.

Despite these positive metrics, the integrity of the cardholder enrolment and authentication process within VbV must be protected for the benefit of all. It is important to ensure that merchants’ investment in 3D Secure is matched by a focus on evolving eCommerce authentication processes; they should stay abreast of, or preferably ahead of, changes in the fraud environment.

To this end, Visa Europe has developed the Visa CodeSure card, an innovative new type of Visa card incorporating a keypad and LCD-screen which is able to generate its own dynamic passcodes. Piloted last year, it has now been launched commercially into the market. Corner Banca in Switzerland has become the first Visa member to commercially launch Visa CodeSure, allowing its Visa cardholders to create a one-time-only passcode for VbV transactions when shopping on merchants’ websites. This next step in authentication technology moves beyond static passwords and ensures that merchants can have confidence that VbV will deliver on its promise of securely authenticating their customers.

Visa Europe is also working with its members to enable them to help consumers better understand and recognise personal security issues as they transact over the internet. By ensuring cardholders are more security aware, they will remain confident of transacting in this space. Clearly, we all benefit from this consumer confidence.

Kevin Smith
SVP Fraud Management, Visa Europe
Merchants Have More Complex Requirements

Today’s automated screening systems may employ interfaces that allow 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 functionality, merchants cannot easily minimise reject rates, review costs or fraud rates. Providing organisations with the ability to adjust business rules in real-time can reduce costs as well as the burden on IT support.

Finance Teams Tend To ‘Own’ Fraud Operations

As per the last survey, finance departments continue to be the principle owner of merchants’ fraud management operations (44%) across small, medium and large organisations (Chart 20). Within very large businesses, this responsibility is likely to sit either with finance (35%) or the operations division (27%); they are also more likely to have a dedicated ‘loss prevention’ function. There is no one correct approach for owning fraud management and the decision should be made based on individual business requirements. Responsibility may be spread across multiple departments and even countries. In these instances, it is even more important to ensure that cross-function communication channels and policies are in place and optimised.

Some 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 world, 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.
Cost of Fraud Management Varies

For the first time, survey participants were asked to approximate how much they will spend on their online fraud prevention and management efforts on an annual basis. The figure includes associated staff, systems and tool costs, but excludes actual fraud losses. For 2010, merchants estimated that they would spend an average of £153,000 (Chart 21), although this varies substantially by size of business. For example, the average for the larger businesses is £249,300. On the other hand, just under half of the smaller companies anticipate spending up to £25,000. Significantly, a high proportion of respondents either didn’t know or were unable to state an answer.

For 2011, around a quarter of respondents anticipate that the cost of fraud prevention and management will increase, with only 10% expecting a decrease (Chart 22). It is worth noting that more digital goods merchants are predicting an increase in total spending (36%) than other business types. Importantly, across all merchant sectors and sizes, the most prevalent response by some margin is that spending will not change in 2011; 59% of businesses provided this response. If budgets are not growing, it is absolutely vital that merchants address their internal fraud management processes, streamlining and boosting efficiencies where appropriate.

The Police Central e-Crime Unit (PCeU) contributes as a critical partner to the provision of a safer and more secure cyber environment in support of the UK National Cyber Security Strategy, working to enhance trust and confidence in the UK as a place to live and conduct business. By improving the police response to victims of electronic crime on both a local and national level we strive to make UK law enforcement fit for purpose in the face of a constantly changing threat, which costs the global economy over a trillion dollars per year.

Over the past twelve months the PCeU has aimed to harness the support of the wider security industry. Our local and international partnerships, with the likes of Europol and the Serious Organised Crime Agency (SOCA), allow us to share resources, intelligence and expertise. This, together with intelligence provided by merchants on suspected fraudsters, has enabled us to identify and prosecute those responsible.

We have also focused on limiting the availability of stolen data, as well as sites where tools and advice are available for online fraudsters. This culminated in the arrest and prosecution of serious organised crime groups and the take-down of a number of websites trading in fraudulent goods and harvesting identities; an area that we continue to investigate.

The multi-geographical nature of e-crime and its crossover with traditional crime means that it remains difficult to quantify. As such, we are currently working with partners and the Government to determine better methods of measuring and reporting such crimes in an effort to provide a more accurate picture of their impact.

During 2011, the PCeU plans to focus on improving law enforcement’s ability to deal with cybercrime, on a national level. This will include the provision of tools to enhance the forensic response of police, thus enabling the successful arrest and prosecution of cybercriminals and fraudsters. We also intend to further invest in collaboration with industry stakeholders to share intelligence and knowledge, and work together to support the fight against e-crime.

Detective Superintendent Charlie McMurdie
Police Central e-Crime Unit (PCeU)
2010 has surpassed industry eCommerce expectations in many ways; online sales channels are continuing to grow in importance as a revenue generator even in times of economic frugality. Importantly, there is also optimism for 2011, with the vast majority of businesses forecasting that their online revenues will increase.

Looking at the key fraud metrics, the survey has found that there is certainly room for improvement. For example, more orders are being accepted post-review than in 2009. Although this increase is not dramatic, the fact that it has not reduced year-on-year should be addressed. Furthermore, the average order reject rate has also grown. Whilst this could indicate that organisations are successfully capturing more suspicious transactions, the proportion of fraudulent orders that are accepted has also risen.

For 2011, there is a focus on achieving more with the same resources; a scenario that is not uncommon in the wider market. Fraud management budgets will remain relatively stagnant, both in terms of the tools being employed and associated staff. Indeed, the vast majority of businesses expect to make no changes to the size of their review teams, even though order volumes are predicted to grow.

With this in mind, merchants should focus on further streamlining internal processes, as well as optimising the use of appropriate anti-fraud tools. Device fingerprinting adoption, for example, remains low, and yet it can play an important role in detecting today’s cleaner fraud. From a process perspective, businesses should build on existing automated screening policies to help ensure that valid orders are not rejected. This is reflected in merchants’ strategic priorities over the next 12 months; respondents stated that enhancing automated detection and sorting capabilities is a top priority.

There are already encouraging signs amongst merchants. Today, a much higher proportion of respondents are using case management systems to support their manual review process, and this is even more apparent amongst larger organisations. Investing in the right fraud systems and processes will provide critical assistance at a time when budgets are tight and businesses are eager to capitalise on the eCommerce opportunity.
CyberSource eCommerce Payment Management Solutions

CyberSource offers a comprehensive portfolio of modular services to help your company manage the entire payment pipeline and optimise sales results. All are available via a single connection to CyberSource.

Global Payment Acceptance

Accept multiple payment types, including worldwide credit/debit cards, regional cards, direct debit, bank transfers and alternative options, 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 data centres located in the US, Europe and Japan. All data centres 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 with deep packet inspection, 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.

---

**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 an effective 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 can also host, support and manage these systems in our secure data centre.

---

**Professional Services**

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

---

**How we can help your business**

The CyberSource Managed Services team can add real value to your fraud screening processes. During 2010, we helped one merchant in the travel industry lower their fraud rate by two-thirds, whilst also reducing the number of bookings requiring manual review by 75%. This simultaneously reduced fraud losses and operating overheads.

The team also worked with a multi-channel retailer to maintain an already low fraud rate on their web channel, whilst cutting the number of website transactions being rejected by over 50%. This led to a reduction in their false-positive rate by offending less good customers, and ultimately boosted sales revenue.

---

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

---

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
CyberSource is more than a global payment gateway – we’re a payment management company. 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 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

United Kingdom

T: +44 (0)118 929 4840

F: +44 (0)118 929 4841

E: uk@cybersource.com

**Americas**

**World Headquarters – USA**

T: +1 650 965 6000

E: sales@cybersource.com

**Asia Pacific**

**Singapore**

T: +65 6499 2000

E: asia@cybersource.com

**Japan**

T: +81 (0)3 5774 7733

E: sales@cybersource.co.jp

**www.cybersource.co.uk**