CyberSource®
the power of payment

Online Payment Fraud Trends, Merchant Practices and Benchmarks

12th Annual Edition

2011 ONLINE FRAUD REPORT

Report & Survey Methodology

This report is based on a survey of U.S. and Canadian online merchants. Decision makers who participated in this survey represent a blend of small, medium and large-sized organizations based in North America. Merchant experience levels range from companies in their first year of online transactions to some of the largest e-retailers and digital distribution entities in the world. Merchants participating in the survey reported a total estimate of more than $65 billion for their 2010 online sales. Survey respondents include both non-CyberSource and CyberSource merchants.

The survey was conducted via online questionnaire by Mindwave Research. Participating organizations completed the survey between September 15th and October 19th 2010. All participants were either responsible for or influenced decisions regarding risk management in their companies.

Summary of Participants Profiles

Online Fraud Survey Wave	2006	2007	2008	2009	2010
Total number of merchants participating	351	318	400	352	334
Annual Online Revenue					
Less than $5M	59%	56%	53%	55%	54%
$5M to Less than $25M	16%	16%	18%	14%	14%
$25M or More	25%	29%	29%	31%	32%
Duration of Online Selling					
Less than One Year	11%	5%	11%	5%	6%
1-2 Years	11%	13%	12%	16%	11%
3-4 Years	18%	18%	13%	14%	19%
5 or More Years	61%	67%	64%	65%	64%
Risk Management Responsibility					
Ultimately Responsible	54%	55%	58%	54%	55%
Influence Decision	46%	45%	42%	46%	45%

Get Tailored Views of Risk Management Pipeline™ Metrics

To get a view crafted for your company's size and industry, please contact CyberSource at 1.888.330.2300 or online at www.cybersource.com/contact_us.

For additional information, whitepapers and webinars, or sales assistance:

- **Contact CyberSource: 1.888.330.2300 or www.cybersource.com/contact_us**
- **Risk Management Solutions: visit www.cybersource.com/products_and_services/risk_management/**
- **Global Payment Solutions: visit www.cybersource.com/products_and_services/global_payment_services/**
- **Payment Security Solutions: visit www.cybersource.com/products_and_services/payment_security/**

Table of Contents

EXECUTIVE SUMMARY **4**

STAGE 1: AUTOMATED SCREENING **7**
- Fraud Detection Tools Used During Automated Screening 7
- Planned Automated Screening Tool Usage 2011 9
- Automated Decision/Rules Systems 10

STAGE 2: MANUAL REVIEW **11**
- Manual Order Review Rates 11
- Review Tools & Practices 13
- Review Operations Efficiency 14

STAGE 3: ORDER DISPOSITIONING (ACCEPT/REJECT) **15**
- Post-Review Order Acceptance Rates 15
- Overall Order Rejection Rates 15
- International Orders Riskier 16

STAGE 4: FRAUD CLAIM MANAGEMENT **17**
- Fighting Chargebacks 17
- Chargeback Management Tools 17
- Chargebacks – Account for Only Half the Problem 18
- Fraud Rate Metrics 19

TUNING & MANAGEMENT **21**
- Maintaining and Tuning Screening Rules 21
- Global Fraud Portals 21
- Merchant Budgets for Fraud Management 21
- Budget Allocation 22

RESOURCES & SOLUTIONS **23**
- CyberSource Payment Management Solutions 23

ABOUT CYBERSOURCE **24**
- For More Information 24

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 summarizes findings from our 12th annual survey.

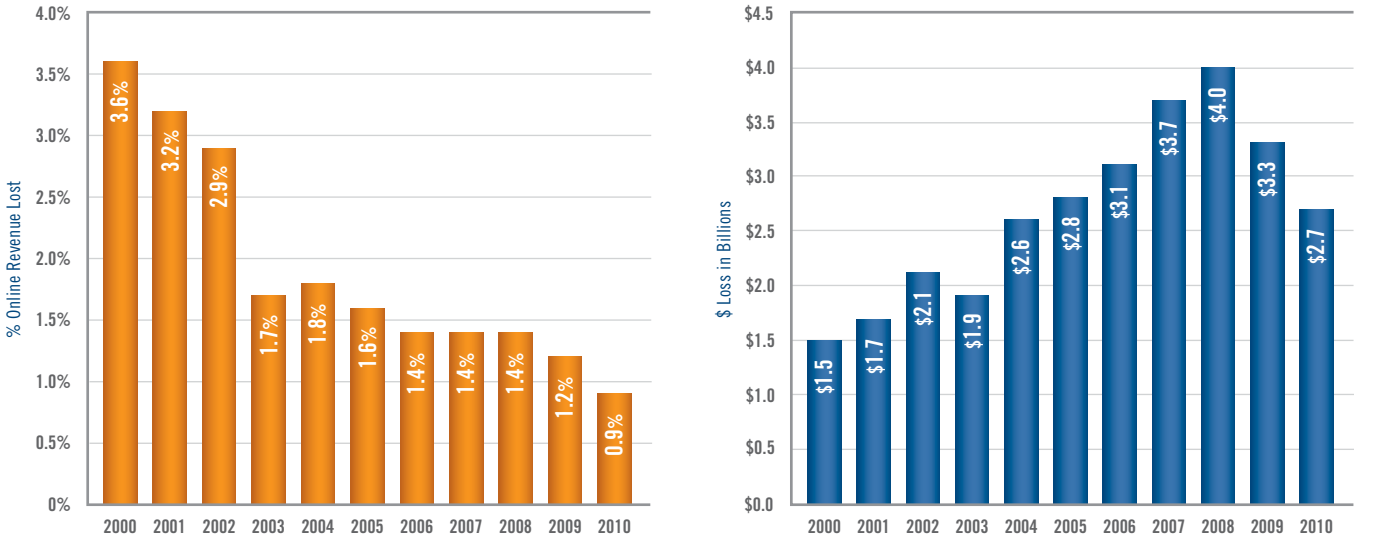
Overview

For the second consecutive year, online merchants improved their fraud management performance. For most of the decade, merchant online fraud losses continued to increase, reaching a peak of $4 billion in 2008. Since that time, merchants have been winning the battle with fraudsters, despite continuing pressure and increasing sophistication of online fraud. In 2008, merchants estimated they lost 1.4% of online revenues to fraud. This revenue loss rate fell to 1.2% in 2009, and in 2010, merchants continued to make progress – reducing fraud losses to 0.9% of revenues, on average. In 2010, fraud pressure (as represented by the sum of the orders merchants reject due to suspicion of fraud, plus the accepted orders that later turn out to be fraudulent) actually increased over 2009 levels. Based on the results of the past two years of the survey, it appears that past investments and experience have allowed many online fraud managers to not only weather the current economic downturn, but also help their online businesses' bottom line performance, by reducing total estimated fraud losses to levels last seen in 2005.

Key Fraud Metrics

The percent of accepted orders which are later determined to be fraudulent did not change significantly in 2010. Merchants reported an overall average fraudulent order rate of 0.9% for their U.S. and Canadian orders, the same as reported in 2009. Over the past seven years, the average percent of accepted orders which turn out to be fraudulent has varied from 0.9% to 1.3%. 2010 represents the second time this rate has dropped below the 1% threshold. The fact that revenue loss rates declined, while fraudulent order rates were relatively stable, may indicate that merchants were more successful managing high dollar fraud attempts in 2010. Among industry sectors, Consumer Electronics reported the highest fraudulent order rate, averaging 1.4%, but this was down from 1.5% in 2009 and 2.0% in 2008.

1



The rate of revenue loss due to online payment fraud declined in 2010 for the second consecutive year, and total dollars lost to fraud declined by an estimated $600 million – returning to levels last seen five years ago.

The share of incoming orders merchants declined to accept due to suspicion of payment fraud increased slightly in 2010, moving from 2.4% to 2.7% of orders, after decreasing for two years in a row. However, this still remains significantly below the 4% average rate seen prior to 2008. The percent of orders rejected due to suspicion of fraud has fallen from 4.2% in 2007 to 2.7% in 2010, a decline of more than 35% in order rejection, representing an increase of 1.5% in total orders accepted.

As the growth of online sales has returned to double digits in 2010, it appears merchants are focusing less on sales conversion and reducing order rejection rates due to suspicion of fraud, and focusing more on continuing to reduce fraud losses. Much progress has been made in the last few years in reducing fraud losses while increasing valid order acceptance, to the point that further gains in both areas may be difficult to achieve and may yield relatively minor contributions to the bottom line. The cost of managing fraud continues to grow in line with the growth of online sales. Historically, the percent of online revenues spent to manage online fraud has been stable. Typically, one-third or more of merchants report spending 0.5% or more of their online revenues to manage fraud.

Chargebacks Understate Fraud Loss by as Much as 50%

This year's survey again probed the percent of fraud losses due to chargebacks. Overall, merchants continue to report that chargebacks accounted for less than half of fraud losses. The remainder occurred when merchants issued credit to reverse a charge in response to a consumer's claim of fraudulent account use. Smaller online merchants reported issuing even more credits in 2010 for fraud claims than in 2009. At the same time 62% of merchants say they perceive that "friendly fraud" has increased over the past two years, as unemployment has risen.

International Order Risk Remains Higher Than Domestic Orders

On average, merchants report the rate of fraud associated with international orders is over two times as high as domestic orders. In 2010, fraud risk on international orders averaged 2.1%. This is similar to 2009 levels, but it is still more than double the fraud rate on domestic orders. However, merchants continued to reject international orders at a rate almost three times higher than domestic orders, and international order rejection rates remained near 7%, on average.

Manual Review Rates

The average percent of orders routed to manual review decreased from 20% in 2009 to 17% in 2010 across all merchants. In some segments, fraud risk is low enough for merchants to rely entirely on automated review, which lowers the aggregate review ratio. But most merchants do manually review some of their orders for fraud risk. In 2010, merchants that performed manual order review saw the average percent of orders sent to review drop from 28% to 24%. This was the third consecutive year manual review rates have declined, even as fraud losses have been reduced.

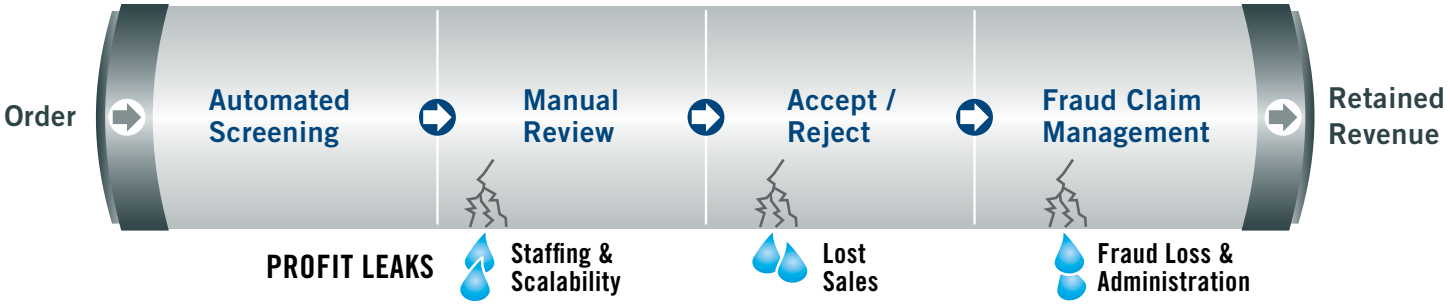
Clearly, many merchants are doing a better job of identifying orders with the highest probability of fraud. Fraud losses have declined, while fewer orders are being manually reviewed. Large online merchants that typically employ more automation continue to have much lower manual review rates. In 2010, large merchants ($25M+ in online sales) performing manual order review reviewed approximately 13% of orders, on average. Merchants continue to rely heavily on manual review teams as a defense against fraud. Historically, half of medium and large online merchants spend, on average, 80% of their fraud management budget on staff. In contrast, the remaining half spent, on average, 27% of their budget on staff, and are managing fraud more cost effectively.

Efficiency Gains Required

As eCommerce sales grow and budgets and resources remain relatively fixed, merchants continue to face the challenge of screening more online orders while keeping order rejection and fraud rates as low as possible, to maximize sales and profits. Continued reliance on manual review presents a serious challenge to processing higher order volumes without adding costs. Can merchants grow their review staff sufficiently to keep pace with fraud? In 2010, 79% of online merchants expect they will not be able to increase manual review staff in the coming year, and 5% expect reductions in staffing. Overall, 81% of merchants anticipate that their budget for fraud management will stay the same or decrease in the next year.

To be successful, many fraud managers will need to adopt tools and practices to make their review teams more efficient. When asked what their top priority was for improving fraud management in the next year, more merchants in 2010 cited streamlining the manual review workflow/process than in 2009. Improving automated fraud detection capability and streamlining manual review processes were mentioned as a top priority by 74% of merchants in 2010, up from 66% in 2009.

Risk Management Pipeline



72% of merchants review orders; these merchants review 24% of orders, on average

47% of fraud management budget is spent on review staff costs

79% of these merchants have no plans to change manual order review staffing during 2011

2.7% Avg. Reject Rate for US/Canadian orders (all merchants)

7.6% Avg. Reject Rate for non-US/Canadian orders (merchants who accept these orders)

0.9% Average Fraud Loss

38% from chargebacks
62% from credits issued

Total Pipeline View

Businesses that concentrate solely on minimizing chargebacks may not be seeing the complete financial picture. Online payment fraud impacts profits from online sales in multiple ways. Besides direct revenue losses, the cost of stolen goods/services and associated delivery/fulfillment costs, there are the additional costs of rejecting valid orders, staffing manual review, administration of fraud claims, as well as challenges 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 (and contain within industry and card brand limits), an end-to-end view is required to arrive at the optimum financial outcome.

In 2010, these "profit leaks" in the Risk Management Pipeline™ impact as much as 21% of orders for mid-sized merchants and as much as 17% of orders for larger merchants – restricting profits, operating efficiency and scalability. This report details key metrics and practices at each point in the pipeline to provide you with benchmarks and insight. Custom views of these benchmarks and practices are available through CyberSource – see page 24 for contact information.

Stage 1: Automated Screening

Fraud Detection Tools Used During Automated Screening

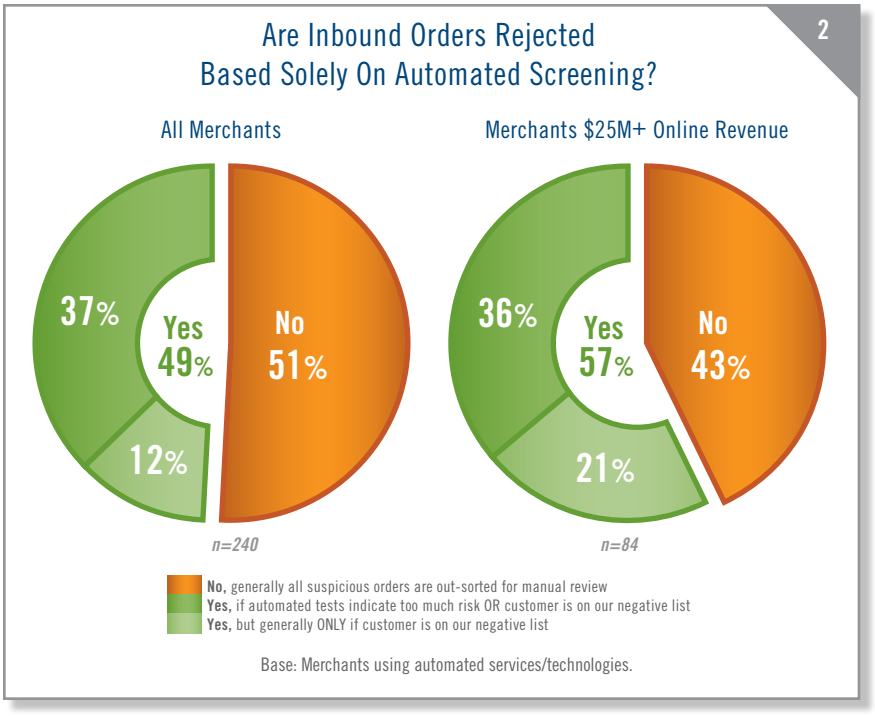
We define detection tools as those used to identify the probability of risk associated with a transaction or to validate the identity of the purchaser. Results of tests carried out by detection tools are then interpreted by humans or rules systems to determine if a transaction should be accepted, rejected 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 to determine if an incoming order might represent a fraud risk. Some merchants will allow this initial automated screen to cancel orders without further human intervention. 49% of all merchants cancelled some orders as a result of their automated screening process and 57% of large merchants indicated they cancelled some orders at this stage (see chart 2).

In 2010, 66% of merchants reported using three or more fraud detection tools for automated screening, with 4.6 tools being the average. Larger merchants dealing with higher order volumes reported using 7.4 detection tools, on average.

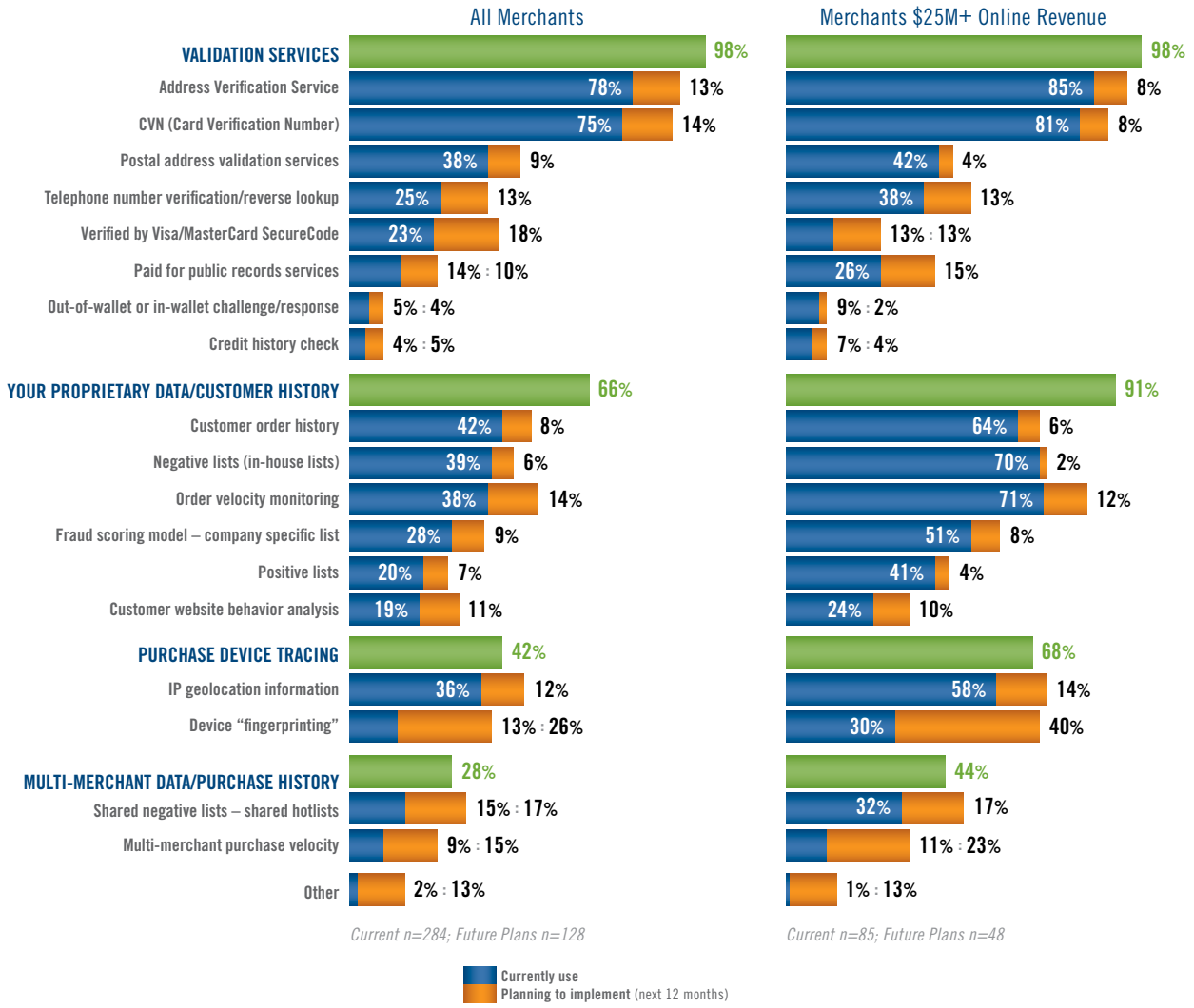
The most popular tools used to assess online fraud risk are shown in chart 3, which shows the current and planned adoption of different tools. Note that the tool usage profile for merchants over $25M in online sales is different than the overall average. These larger merchants generally use tools across all four dimensions of detection, and more often use their customer history and proprietary data during the automated order screening process. They have a higher use of company-specific risk scoring models, negative and positive lists, and sophisticated order velocity monitoring tools.

Overall, 98% of merchants use one or more validation tools. These tools are often provided by the card brands to help authenticate cards and cardholders. The tools most often mentioned by merchants are the Card Verification Number and the Address Verification Service (AVS). AVS compares numeric address data with information on file from the cardholder's card issuing bank. AVS is generally available for U.S. cardholders and for limited numbers of cardholders in Canada and the United Kingdom. AVS is subject to a significant rate of "false positives," which may lead to rejecting valid orders, as well as missing fraudulent orders. If the cardholder has a new address or a valid alternate address (such as seasonal vacation home), this information may not be reflected in the records of the cardholder's issuing bank, so the address would be



3

Fraud Detection Tool Current Usage and Plans



flagged as invalid. Merchants typically do not rely solely on AVS to accept or reject an order.

The Card Verification Number (CVN – also known as CVV2 for Visa, CVC2 for MasterCard, CID for American Express and Discover) is the second most commonly used detection tool. 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 card verification number during an online purchase can add a measure of security to the transaction. However, CVNs can be obtained by fraudsters just as easily as credit card numbers. CVN usage by online merchants has significantly increased in the last five years, rising from 44% in 2003 to 75% today.

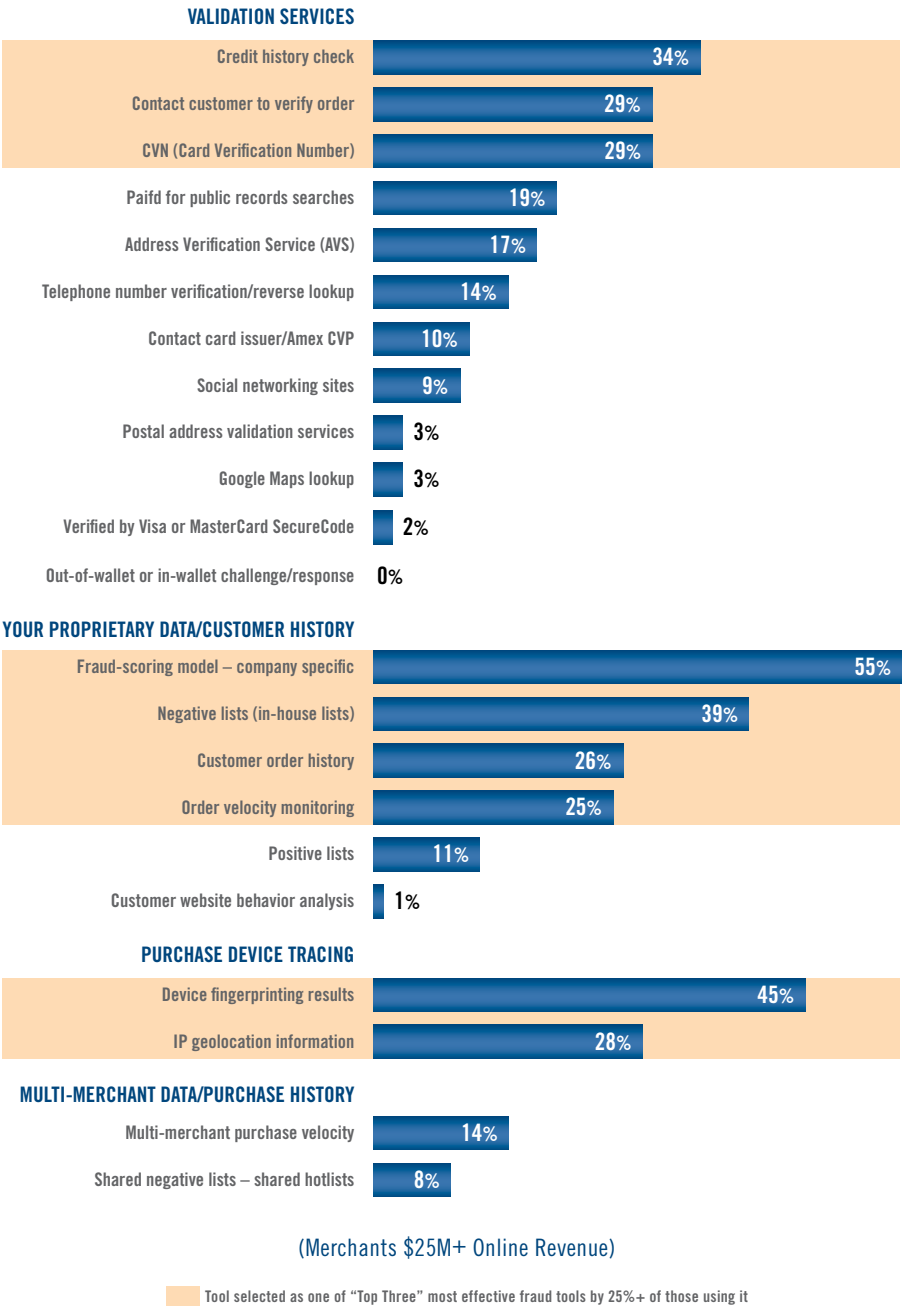
Large merchants were asked to identify the three most effective tools they use. To eliminate the bias that could stem from more commonly used tools receiving more mentions, we normalize the data by looking at the percent of merchants using a particular tool, who cite that tool as one of their top three choices.

Company specific fraud screens received the highest effectiveness rating by merchants who use this tool. Over half of large merchants use custom fraud models, and 55% of these merchants rated them as one of their three most effective tools. These fraud screens are risk scoring models which are tuned using an individual merchant's historical data on factors associated with online orders. Since fraudsters learn over time and vary their strategies,

4

Most Effective Fraud Management Tools

% merchants using tool that selected it as one of their "top three" most effective*



(Merchants $25M+ Online Revenue)

Tool selected as one of "Top Three" most effective fraud tools by 25%+ of those using it

** Base: Merchants with annual online sales ≥$25M who use tool : automated or manual (excludes None)*

we typically find most risk scoring models need regular tuning with new analysis and data in order to maximize their effectiveness.

More large merchants are adopting device fingerprinting technology to help detect online fraud. In 2010, 30% of large merchants report using this technology, up from 18% in 2009. Of the merchants using device fingerprinting, almost half (45%) rated this tool as one of their three most effective for managing fraud, making it the second highest rated tool for effectiveness. Custom-built negative lists were used by 70% of large merchants and was rated as the third most effective tools, with 39% of those merchants selecting it. Half of the larger merchants also employ IP geolocation tools in their fraud management process. IP geolocation tools attempt to identify the geographic location of the device from which an online order was placed. It provides an additional piece of information to compare against other order information and order acceptance rules, to help assess the fraud risk of an order. In some cases, only an Internet service provider's address is returned, so the ultimate geographic location of the device remains unknown. Fraudsters may also employ anonymizers/proxy servers to hide their true IP address and location.

Planned Automated Screening Tool Usage 2011

Device Fingerprinting Highest on "Plan to Buy" Lists

Thirty-nine percent of the surveyed merchants planned to add one or more new fraud detection tools to their automated screening process over the next twelve months. Device fingerprinting, and payer

authentication services provided by the card brands are the two tools having the highest level of planned adoption over the next year.

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 set of devices. Overall, 26% of merchants report plans to add device fingerprinting in the next twelve months and 40% of large online merchants indicated they were planning to add device fingerprinting.

As in the past several years, card brand payer authentication services (e.g. Verified by Visa, MasterCard SecureCode) figure prominently in merchants' future plans. 2010 survey results show that 23% of merchants currently use one or more of the available payer authentication services. Currently, 18% of respondents say they are interested in deploying these systems in the next twelve months as a new tool to manage fraud.

Implementing payer authentication should reduce exposure to card-not-present fraud loss either by authenticating the buyer's identity or by shifting fraud liability back to the card issuing bank (interchange incentives also apply). Further, certain card types in some countries are beginning to require that payer authentication solutions be used as a condition of accepting the associated cards (e.g. Maestro Cards in the United Kingdom). But if merchants have a sufficiently high direct fraud loss rate, the card brand may not permit the merchant to shift liability, even if the merchant has implemented a payer authentication system. These systems may help reduce the incidence of online credit card fraud, if a critical mass of consumers register their cards and accept the new checkout procedures.

Successful adoption of payer authentication will require merchants to put procedures in place to handle customers who have not adopted verification services or who use cards or payment types which are not supported. International expansion and the growing popularity of online payment types such as electronic checks, PayPal™, Bill Me Later®, etc. also drive the need for alternative fraud management techniques.

Automated Decision/Rules Systems

Automated Order Screening

Automated order decisioning/screening systems continue to grow in use and are now used by 67% of merchants (up from 25% in 2005) and 89% of large online merchants. These tools help companies automate order screening by applying a merchant's business rules in the real-time evaluation of incoming orders.

Decision and rules systems automate the evaluation of test results generated by fraud detection tools, and determine whether the transaction should be accepted, rejected, or suspended for review. As the number of tools used grows, it is becoming increasingly important for merchants to employ automated systems to interpret and weigh the multiple results for each product or transaction profile (versus a "one size fits all" screen), to optimize business results. The introduction of new products, services or markets often requires a unique set of acceptance rules, and because fraud patterns are dynamic, it is imperative that these systems quickly adapt to the changing environment. Sixty percent of large merchants say their screening system allows business managers to create and modify screening rules without assistance from external experts or internal information technology (IT) staff.

Results of Automated Screening

The automated order screening process generates three outcomes: 1) order acceptance without further review; 2) orders flagged for further review; and 3) automatic order rejection. Forty-nine percent of merchants indicated they reject some orders based on automated screening tests, and 57% of large merchants indicated doing so.

Stage 2: Manual Review

Orders which do not pass 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.

Manual review represents a critical area of profit leakage. It is expensive, limits scalability, and can impact customer satisfaction. For many merchants, it represents half of their fraud management budget. Only 16% of merchants say they have budget available to increase review staff now or in the next twelve months. This presents significant challenges to profit growth, since the total number of orders that must be reviewed increases in step with the total increase of online sales, even at a stable percent of orders sent to review.

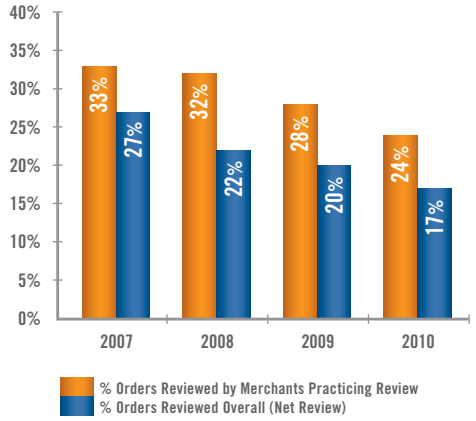
Manual Order Review Rates

In what should be a highly automated sales environment, most merchants are manually checking orders. However, over the past four years, the survey data shows merchants have made some progress in reducing the rate of manual review from 27% of orders overall in 2007 to 17% in 2010. Merchants who conduct manual reviews are now reviewing, on average, 1 out of 4 orders, down from 1 out of 3 in 2007. Merchants of all sizes use manual review to manage payment fraud. Chart 6 shows smaller merchants review a higher percentage of orders (perhaps because lower order volumes permit such practice) but even larger merchants review a significant percentage of online orders and likely devote more resources to this task than is operationally scalable.

5

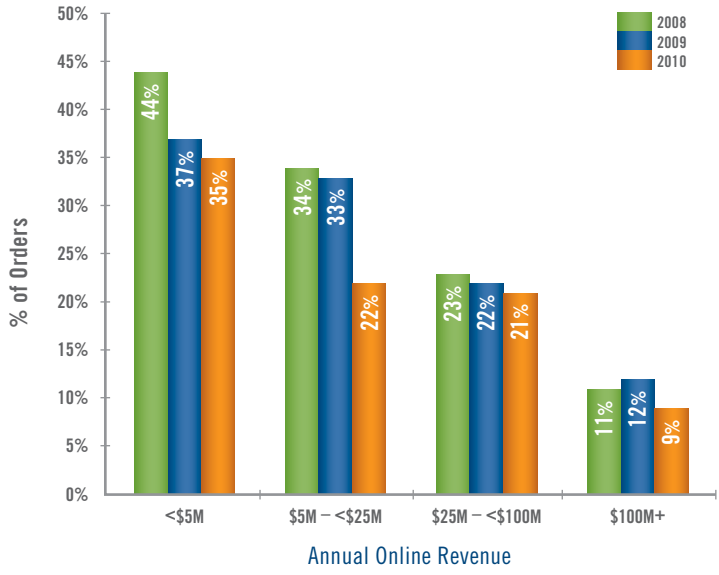
Manual Review Trends

Over the past 4 years, manual review rates have declined. However, online merchants performing manual review still review on average 1 out of every 4 orders received.



6

Average % of Orders Manually Reviewed
(for merchants engaged in review)

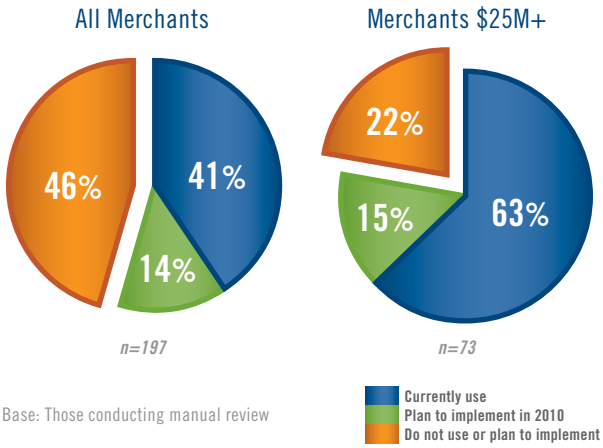


One consequence of using more fraud detection tools during automated screening is a greater chance of one or more flags being raised, resulting in an order being selected for manual review. Adding more tools to detect fraud may result in downstream impacts and costs, if these tools are not carefully integrated into a merchant's review process and tuned to a merchant's specific situation.

Merchants expecting increased online sales will need to take at least one of the following actions: 1) divert more staff time to the order review process; 2) increase staffing levels; 3) allow more time to process orders and ship good ones; or 4) improve accuracy of initial automated sorting and make the subsequent review process more efficient.

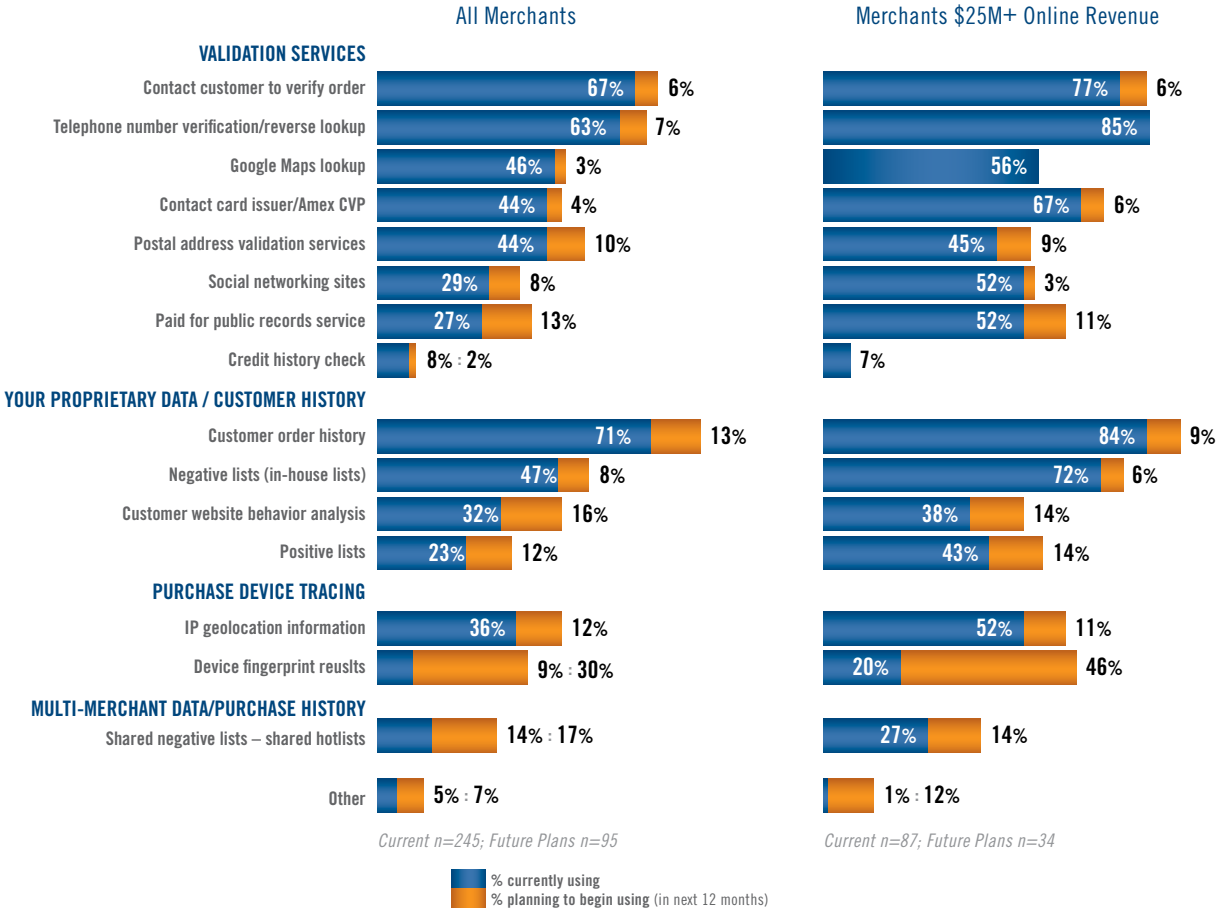
7

Use or Plan to Implement Case Management System to Support Manual Order Review Process



8

Fraud Detection Tool Usage During Manual Review



Review Tools & Practices

Given the reported limitations on hiring additional manual review staff, there is increased focus on investing in tools and systems to increase the productivity and effectiveness of review staff. While the primary focus should be on improving initial automated sorting accuracy to decrease need for review, attention to streamlining the review process is also warranted.

Use of Case Management Systems

Currently, 4 out of 10 merchants report having a case management system that supports their manual review process and staff. Fifty-five percent of merchants either currently use a case management system or plan to implement one in 2011. Large online merchants have rapidly adopted case management systems, with 63% currently using them, up from 39% just two years ago. Almost 8 out of 10 large merchants currently use or plan to implement a case management system.

Merchants using a case management system are also more likely to be able to track fraud rates on orders which have gone through manual review. 69% of merchants using case management systems report tracking fraud rates for manually reviewed orders.

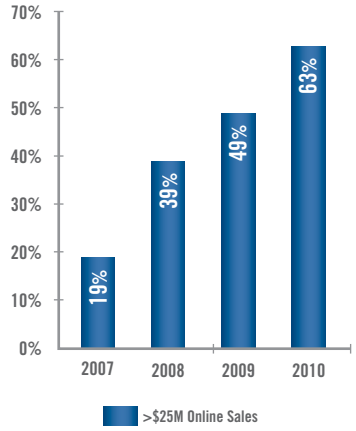
Overall, 48% of merchants performing manual order review say they do not track the fraud rates of orders which have been manually reviewed, and one-third of large merchants report not being able to track this information. Without knowing the fraud rate on orders going through manual review, and who reviewed them, it is difficult to determine training needs or other actions to improve the effectiveness of manual review.

Tools Used/Planned During Manual Review

While many of the tools or detector results used during automated screening can also be used during manual review, several additional tools and processes are employed by manual reviewers. Attempting to validate an order by reviewing past customer order history and contacting the customer is standard practice for 7 out of 10 merchants overall, and 8 out of 10 large merchants. However, most organizations have policies regarding how quickly they must clear orders through manual review and how long they will wait for customers to respond to requests for additional information. Most merchants try to clear orders through manual review in one business day and say they will not wait more than three business days for a customer to respond to a request for more information. Another practice used only in manual review is to contact the card issuer. This action is taken by 44% of merchants overall and 67% of large merchants. Telephone number validation/reverse lookup is the third most popular tool with 63% of merchants using it during manual review versus 25% during automated screening. Large online merchants are more likely to maintain and use negative lists during both automated screening and manual review processes.

9

Adoption of Fraud Case Management Systems by Large Online Merchants



This year, we also asked about using Google Maps to investigate street and aerial views of delivery addresses, and researching suspicious buyers using social networking sites. Google Maps was used by 46% of all merchants and 56% of large merchants, and ranked fifth in adoption, just behind in-house developed negative lists. The use of social networking sites to research suspicious buyers was used by 29% of merchants and 52% of large merchants. This level of adoption was very similar to reported usage of "paid for public records services," so perhaps data in social networks supplements traditional background checks. In 2010, over half of merchants reported using 5 or more fraud detection tools for manual review, with 5.7 tools being the average. Larger merchants reported using 7.8 detection tools, on average.

The most popular tools currently used in the manual review process are shown in chart 8, including the percent of merchants planning to add each tool in 2011. Utilizing the information produced by device fingerprinting technology during the manual review process is the main focus of most merchants over the next year.

Review Operations Efficiency

Reviewer Efficiency

The median number of orders a reviewer processed in a day ranged from 5 for small merchants to 100 for large merchants, with an overall median of 50 orders per day (see chart 10). The rate is down slightly from 2009 and may reflect the fact that a lower percentage of orders are being out-sorted for manual review, allowing reviewers to spend more time investigating the truly suspicious and higher risk orders. Large merchants who typically have case management systems achieve 100% higher throughput per reviewer in the manual review stage, possibly due to greater use of review systems and detection tools during manual review. Typically, reviewers spent 9.5 minutes reviewing an order in 2010, up from 8 minutes in 2009.

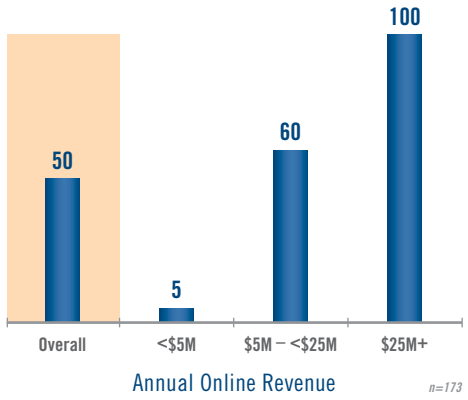
Merchants reported that reviewers were required to invoke and input data to 4.0 systems to review an order on average, up from an average of 3.7 in 2009. The ability to integrate or automate interfacing with these multiple systems represents an opportunity to further streamline the review process and increase reviewer productivity and effectiveness.

Staff Tenure

Given the cost and time required to recruit and train new staff, merchants need to focus on staff retention. Fraud rates or order rejection rates can increase if highly experienced review staff leave an organization and are either not replaced or replaced by less experienced reviewers.

10

Median # Orders Reviewed Per Day/Reviewer
(by merchant size)



Final Order Disposition

Automated screening and manual order review ultimately result in order acceptance or rejection. A relatively high percentage of manually reviewed orders are ultimately accepted (see next section) – highlighting the need for merchants to continue to improve automated screening accuracy and reduce the need for review. A look at order reject and acceptance rates follows in Stage 3 of the pipeline review.

Stage 3: Order Dispositioning (Accept/Reject)

Post-Review Order Acceptance Rates

Over the past few years, merchants who manually review orders indicated they ultimately accepted approximately 75% of the orders they manually reviewed (see chart 11). In 2010, the average rate of acceptance for orders going through manual review remained high at 76%. Fifty-five percent of merchants report they accept 90% or more of the orders they manually review. These merchants are incurring significant expense to find the 10% of the review queue they believe to be too risky to accept. Clearly, most merchants require better methods to determine the orders to be outsorted for manual review, so only truly suspicious orders receive human attention.

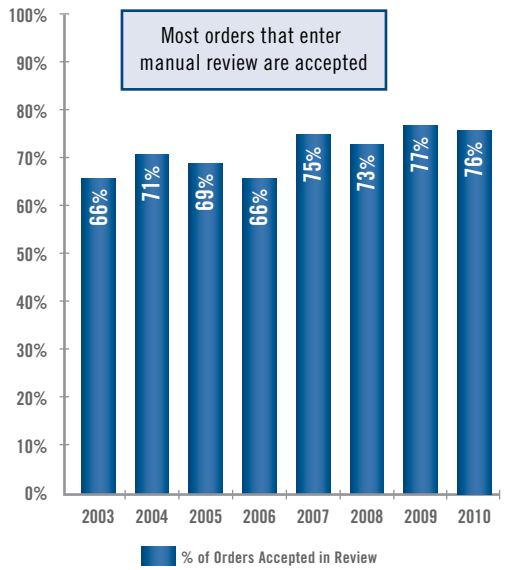
Order acceptance rates in the manual review stage are uniformly high across all merchant online sizes. In fact, the largest online merchants had the highest average order acceptance rates in 2010, as chart 12 shows.

Overall Order Rejection Rates

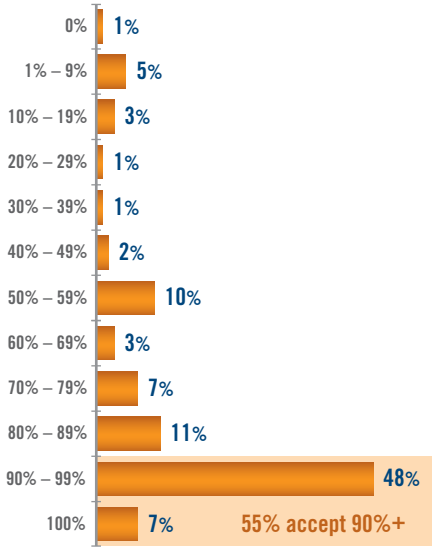
Order reject rates can reflect true fraud risk or signal "profit leaks" in terms of valid order rejection or unnecessarily high rates of manual review. In 2008, for the first time in several years, merchants participating in the survey reported a significant drop in their order rejection rates, from 4.2% in 2007 to 2.9% in 2008 (see chart 15) and the rate continued to fall in 2009.

11

Post-Review Acceptance Trends



% of Merchants Reporting This Level of Post-Review Acceptance

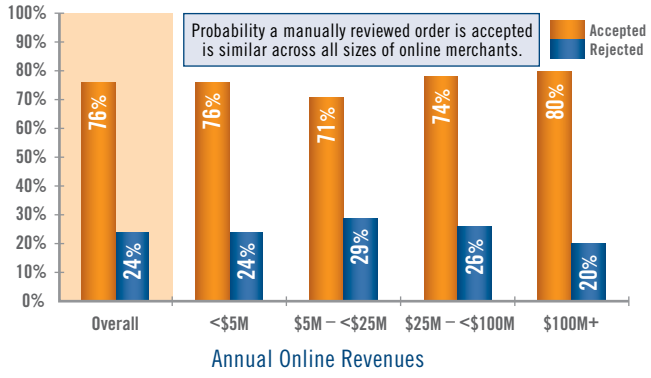


In 2010, large merchants continued to make progress in reducing rejection rates and increasing order acceptance rates in their fraud management process while medium and small merchants reported increases in order rejection rates. Overall, the average order rejection rate in 2010 increased to 2.7% up from 2.4% in 2009. In 2010 order rejection due to suspicion of fraud increased for most types of merchants but decreased for Consumer Electronics sellers and Health & Beauty categories (see chart 14).

As double digit growth returns to online sales it appears many merchants are willing to let order rejection rates increase in order to further reduce fraud losses. Depending on a merchant's cost of goods and other factors, profits

12

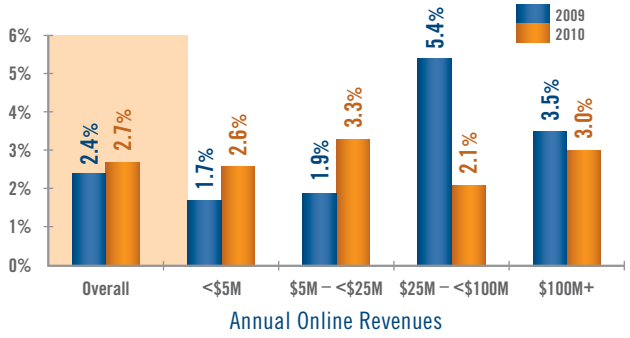
Average % of Manually Reviewed Orders that are Accepted/Rejected



Base: Merchants practicing manual review (excludes None/No answer)

13

Average % Orders Rejected Due to Suspicion of Fraud



may be maximized by accepting a slightly higher level of fraud if offset by lower order rejection rates and reduced customer insults.

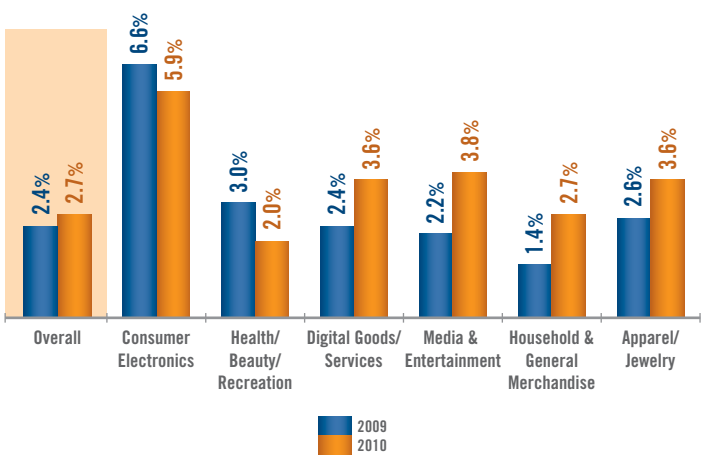
Order rejection rates also vary by type of product and merchant profile. Chart 14 shows that segments which have high cost of goods sold and/or lower gross margins tend to have higher order rejection rates. Each fraud loss in this arena has a large negative profit impact. Consumer electronics and jewelry/apparel are two examples of online segments that tend to have higher-than-average order rejection rates. Yet even within similar groups of online merchants, we see that some merchants achieve low order rejection rates while still keeping fraudulent order rates under control. Examining the large consumer electronics merchants in the sample, we find that over half of these merchants report order rejection rates of 3% or less, while maintaining fraudulent order rates at or even below the average for their segment.

International Orders Riskier

Merchants consistently report a much higher level of order rejection on international orders due to suspicion of payment fraud. In 2010, merchants report their rejection rate on these orders is almost triple that of domestic orders, as shown in chart 15. After making significant progress in reducing order rejection rates for international orders from 2006 to 2009, merchants report no significant change in international order rejection rates in 2010. The actual fraud rate experienced on international orders supports a cautious approach to order acceptance, as merchants report the fraud risk on international orders is significantly higher than that of domestic orders.

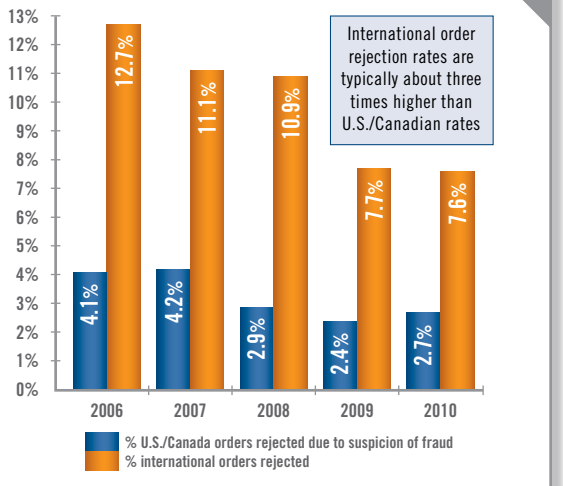
14

Order Rejection Rates by Selected Online Segment



15

Order Rejection Trends



Stage 4: Fraud Claim Management

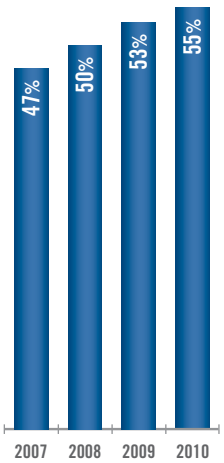
Fighting Chargebacks

Inevitably, some orders are accepted that later turn out to be fraudulent. Merchant practices vary with respect to how fraudulent orders are handled, so it is important to understand online merchants' practices associated with reviewing and contesting chargebacks ("re-presentment"). For several years, the share of fraud-coded chargebacks merchants contest has increased from 47% to 55% in 2010. Large merchants increased the portion of fraud chargebacks they contested from 49% to 62%, on average. However, when we look at the distribution of merchants' answers to this question, we continue to find that over one third of merchants are disputing 90% or more of their fraud chagebacks, while 2 out of 10 merchants are disputing less than 10% of their fraud chargebacks (see chart 16).

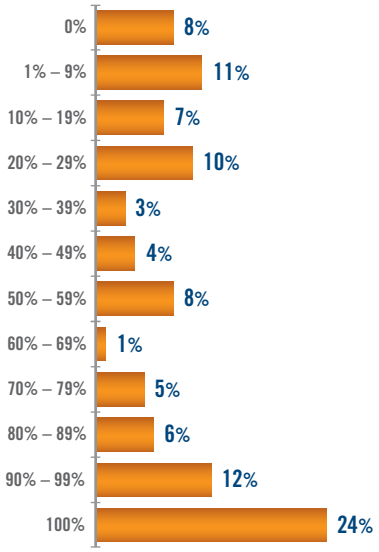
Merchants report that they win 41% of the chargebacks they dispute, on average. Over the past five years, the average chargeback win rate has ranged from 40% to 44% of chargebacks re-presented by merchants. Simply using the average percent of chargebacks that are disputed (55%) multiplied by the average win rate of 41% results in a net recovery rate of 23% (meaning 23% of all fraud-coded chargebacks are recovered). However, given the wide disparity in the chargeback re-presentment rate, when these are calculated on a merchant-by-merchant basis and then averaged, the re-presentment win rate rises to 24% (see chart 17). This is the same chargeback recovery rate as reported in the 2009 survey. Disputing most fraud chargebacks and having an efficient re-presentment process can enhance profitability and reduce fraud loss.

16

Average % Total Fraud-Coded Chargebacks Re-presented



% of Merchants Reporting This Re-presentment Rate

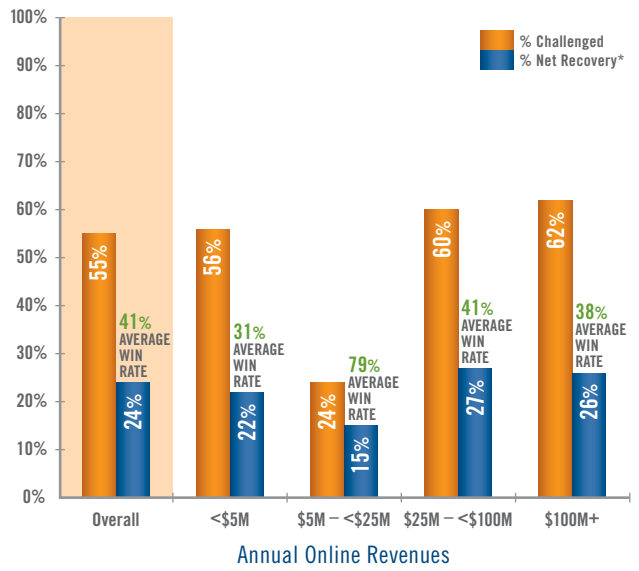


Chargeback Management Tools

Of course, disputing chargebacks is not an easy nor cost-free process. Merchants must manage and organize all order, delivery and payment information to successfully dispute fraudulent orders with financial institutions. Merchants have adopted automated systems for handling this aspect of the pipeline. In 2010, 63% of large merchants reported using these tools. In previous surveys, we asked merchants to provide estimates of how many hours it takes on average to handle a fraud chargeback. The average time spent overall was 1.8 hours, with a median time of 1 hour to handle a fraud chargeback (total time consumed for research, documentation, submission). The largest merchants reported a median time of 30 minutes per fraud chargeback. Clearly, fraud chargeback management is a significant expense for merchants. However, having automated chargeback tools that facilitate contesting fraud chargebacks can pay off, as merchants often win a significant portion of fraud chargebacks when correctly re-presented.

17

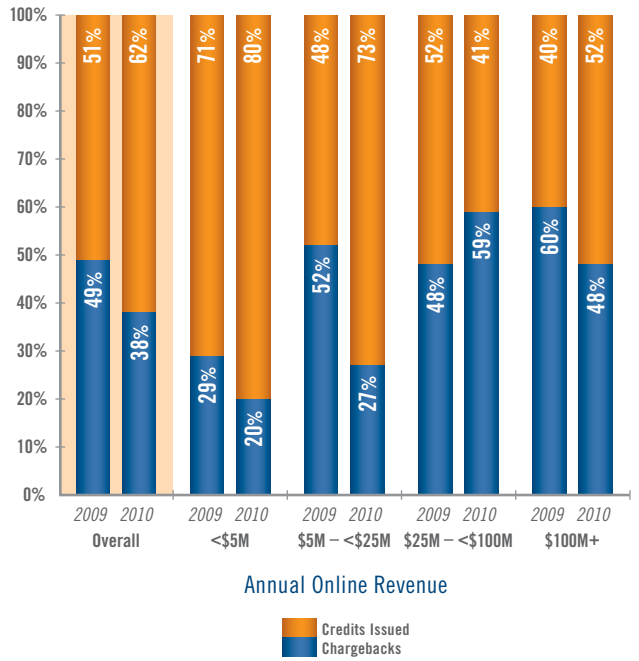
Fraud Chargeback Re-presentment: Win Rate/Net Recovery Rate



*(*Net Recovery Rate is expressed as a % of all fraud-coded chargebacks challenged)*

18

% of Fraud Claims: Chargebacks vs. Credit Issued by Merchant 2010 vs. 2009



Chargebacks – Account for Only Half the Problem

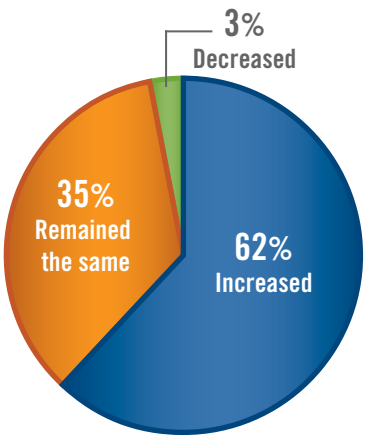
How a fraudulent order is handled can have a significant impact on bottom line profits. Fraudulent orders are presented to the merchant via two main routes: as a chargeback or as a direct request from a consumer for credit (they claim fraudulent use of their account). Although chargebacks are the most often cited metric, merchants report that chargebacks actually account for less than half of all fraud claims.

In 2010, large merchants ($25M+ online sales) reported that just over half of their fraud was presented in the form of a fraud-coded chargebacks (see chart 18), similar to 2009 levels. However, small and medium online merchants reported that the credits they issued in response to fraud complaints accounted for a larger proportion of their fraud losses in 2010. This resulted in the overall average share of fraud losses due to chargebacks dropping from 49% of fraudulent orders to 38%.

Considering the financial impact of both fraud claim routes (chargebacks and credit issuance/reversal), some merchants encourage direct consumer contact to address fraud claims and thus avoid the additional chargeback fees levied by the merchant bank/processor. If a consumer contacts the merchant first, then the decision is in the merchant's control to either handle the dispute directly with the consumer or to advise them to initiate a fraud chargeback process. In any event, if merchants are evaluating fraud losses solely on the basis of chargebacks, the actual rate of fraud loss the business is experiencing may be as much as two times higher, due to direct credit issuance/charge reversal. Part of the rise in fraud losses from issued credits to avoid chargeback claims may stem from a perceived increase in the levels of "friendly fraud," where a buyer may receive goods or services but denies making the purchase or receiving the goods. In some instances, the order may have been made by a family member or friend, hence the term "friendly fraud." Larger merchants with broader customer bases may be more likely than smaller merchants to have proof of delivery records or insist that customers file a formal affidavit and fraud claim with the appropriate payment service provider. Chart 19 shows that, as unemployment has increased, 62% of merchants believe that "friendly fraud" has increased over the past two years.

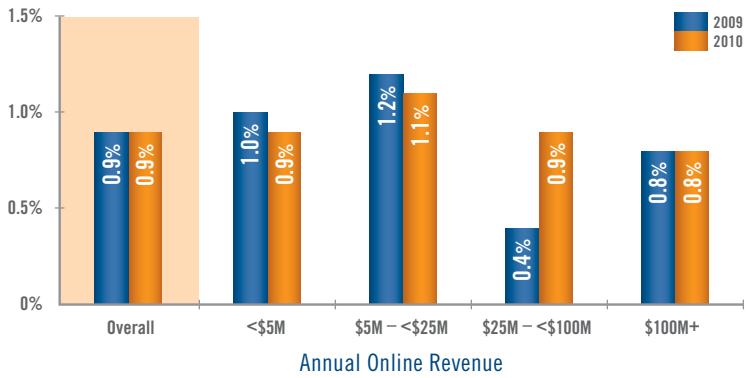
19

Change in "Friendly Fraud" Over the Last 2 Years



20

Average % Accepted Orders Resulting in Fraud Losses



A fraud chargeback was received on the orders OR a credit was issued directly to a customer who claims not to have placed an order

Fraud Rate Metrics

When monitoring the level and trend of online fraud loss, we focus on three key metrics: 1) Overall revenue lost as a percent of total online sales; 2) percent of accepted orders which turn out to be fraudulent (domestic and international); and 3) the average value of a fraudulent order relative to a valid order. Fraud rates vary widely by merchant and depend on a variety of factors, such as online sales volume, type of products or services sold online, and how such products/services are delivered and paid for. It is important that merchants track key fraud metrics over time and evaluate their performance relative to their peer group (both size and industry).

Note: this report provides benchmarks on total fraud rates (chargebacks + credits issued directly to consumers by merchants). As such, these metrics tend to be higher than those reported by banks and credit card brands, which generally base reported rates on chargeback activity only.

Depending on the products or services being sold online, fraud loss risk tolerances and order rejection rates can vary significantly. Merchants selling high cost goods with relatively low gross margins, like most consumer electronics products, tend to err on the side of rejecting more orders to avoid expensive fraud losses. Merchants who are less subject to fraud attacks can achieve similar fraud loss rates while rejecting relatively few orders.

Direct Revenue Loss Rates

Very large merchants typically use more tools and have more experience and resources to manage online fraud, so their fraud rates tend to be lower than the overall rate. Revenue loss measurement includes not only the value of orders on which fraudulent chargebacks are received, but also the cost of any credits issued to avoid such chargebacks. In 2010, the average percent of online revenues lost to payment fraud ranged from 1.1% for small merchants to 0.4% for the very largest merchants (more than $100 million in online sales). Fraudsters often target medium size merchants ($5 million to $25 million in online sales), since these merchants have enough online order volume to allow multiple fraud attempts, but may not yet have the fraud management experience nor dedicated people or systems in place to defend against professional fraudsters.

Fraudulent Order Rate for Accepted Orders

Another key metric is the number of accepted orders that later turn out to be fraudulent. This rate is expressed as a percent of total accepted orders. Chart 20 shows the average fraudulent order rates by online revenue size. Overall, 29% of merchants reported a fraudulent order rate of 1% or more in 2010.

International Orders Carry Higher Risk

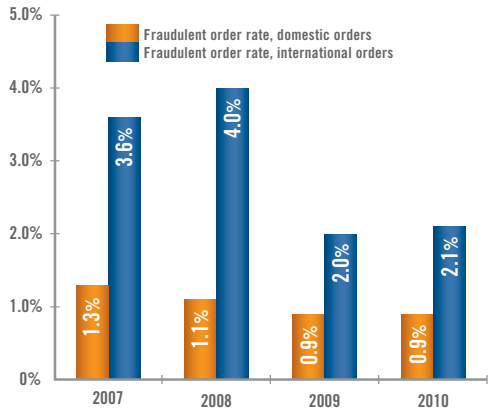
Over the past two years merchants have made significant progress in managing fraud risks associated with international orders. Fifty-three percent of merchants surveyed accepted orders from outside the U.S. & Canada in 2010. International sales accounted for an average of 20% of total orders for these merchants, similar to 2009 levels. This same group reported that the actual

direct fraud rate on international orders fell from 4% in 2008 to an average of 2.1% in 2010, so many merchants are improving their fraud management performance on international orders.

Of course, online merchants must still make sure that their fraud detection and management systems are robust enough to handle the additional risk involved. Despite progress made, international orders still have twice the overall fraud rate of domestic online orders. Some merchants say they've even stopped accepting orders from some countries, in order to manage international fraud. Of the merchants who accepted international orders in 2010, one out of five stopped accepting orders from one or more countries in the past year due to high fraud levels.

21

Domestic vs. International Fraud Rate Trends



Merchants who sell online outside of the U.S. & Canada report that they reject international orders due to suspicion of fraud at a rate that is almost 3 times the U.S. and Canadian average rate – rejecting approximately 1 out of every 13 international orders received (see chart 15).

Average Value of Fraudulent Order Higher than a Valid Order

Historically, fraudulent orders tend to have higher values on average than valid orders. In 2010, the median value of a fraudulent order was $245, compared to a $120 median value reported for valid orders. Since fraudulent orders tend to be somewhat higher in value than valid orders, merchants will tend to outsort more high value orders for manual review and verification.

Tuning & Management

Maintaining and Tuning Screening Rules

Compared to the previous survey, even more merchants reported that the fraudulent orders they experienced in 2010 were "cleaner" than those they experienced just 12 months before. By "cleaner," we mean they have fewer anomalies–they look more like valid orders than ever before.

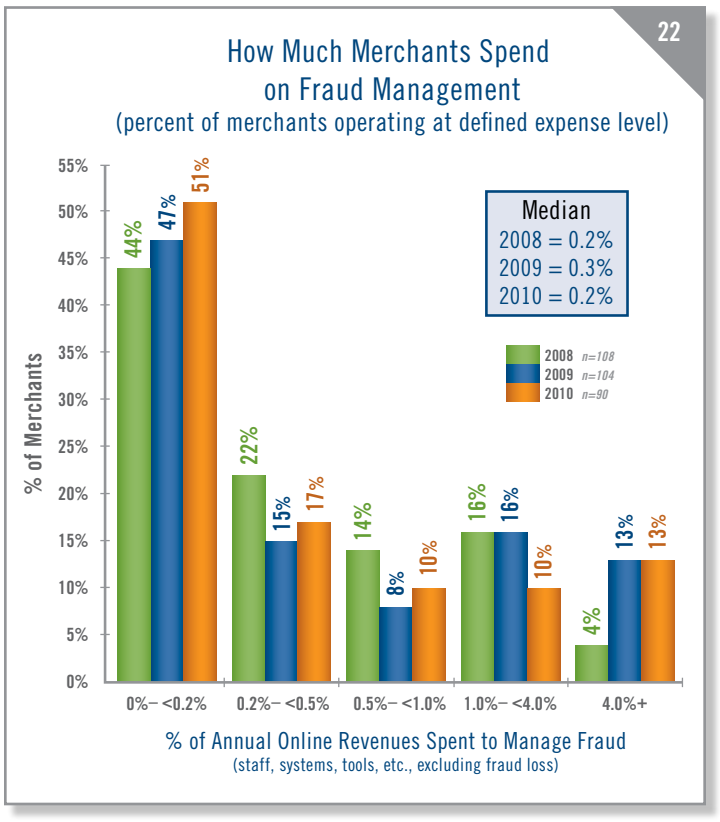
Fraudsters' growing use of botnets may be a key factor in "cleaner" fraud. Botnets allow fraudsters to more deftly mimic the identity of a true customer and mask their own identity. Therefore, it will be increasingly important for merchants to deploy technologies to identify botnet attacks and operate systems that rapidly respond to new fraud patterns and trends. Forty-two percent of merchants say they now have an automated order screening system in place that allows business managers to modify decision rules without assistance from internal IT staff or external parties (up from 16% found in 2006). The ability to adjust automated order screening systems quickly helps 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 minimize reject rates, review costs, or fraud rates. Additionally, giving business managers the capability of adjusting business rules on-the-fly reduces the costs and burden of IT support.

Global Fraud Portals

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 being integrated with these portals, with accompanying enhancements to streamline workflow. Global fraud portals ideally include hierarchical management, as companies strive to centralize fraud management across multiple lines of business and geographies.

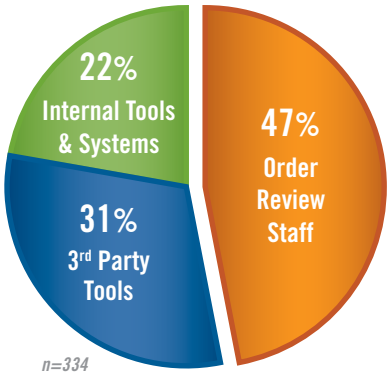
Merchant Budgets for Fraud Management

How much are online merchants spending to mitigate fraud risk? In 2010, survey results show that 33% of merchants spend 0.5% or more of their online revenues to manage online payment fraud, while 67% spend less than 0.5%. In 2010, the median ratio of fraud management expense to sales was 0.2% across all merchants, although some merchants in high risk categories are spending significantly more. These spending estimates focus on the cost of managing fraud risk (internal and external systems and services, management development, and review staffs). Direct fraud loss (chargebacks, lost goods and associated shipping costs), as well as the opportunity cost associated with valid order rejection, are not included here (see chart 22).



23

Average % Spending Allocation for Fraud Management 2010



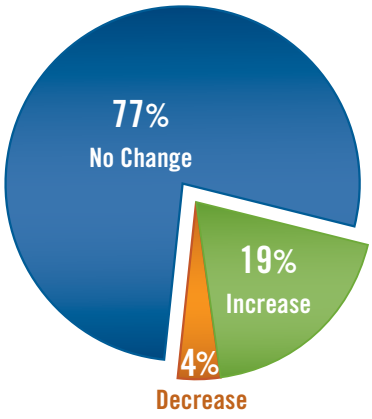
Planned Review Staffing Levels

	Increase	Same	Decrease
2011	16%	79%	5%
2010	13%	78%	9%

Base: Those with 1 or more full-time manual review staff

24

Expected Budget Change for Fraud Management 2011

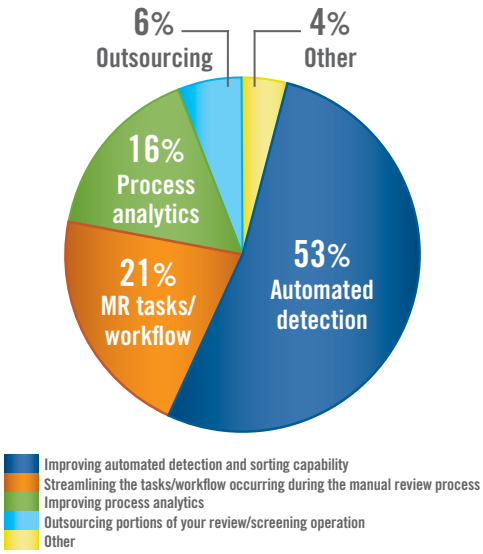


Average % Fraud Management Budget Expected to INCREASE: 10%

Average % Fraud Management Budget Expected to DECREASE: 25%

25

Top Priority Strategy/ Area of Focus



Budget Allocation

For many years, merchants have consistently spent just over half their fraud management budgets on review staff. However, the survey shows a shift of deploying more budget towards using external third party tools and services in 2010. Merchants report that 31% of their budget on average is allocated to these tools, up from 24% in 2009 (see chart 23). The remainder is allocated for manual review staff (47%) and on internally developed tools and systems (22%).

Clearly, review staff costs remain the dominant factor and only 16% of merchants cite plans to increase review staffing in 2011. Over three-fourths of merchants expect budgets for fraud management in 2011 will remain the same (or decline), as compared to 2010 (see chart 24).

Reducing the need for manual review and increasing the efficiency and effectiveness of reviewers is key to growing online business profits and managing the total cost of online payment fraud. One place to start is by improving the automated detection of risky orders to reduce manual order review volumes. When asked about their top priority strategy or area of focus for process improvement in 2011, 53% of merchants said improving the automated detection and sorting capabilities of their systems was their key area of focus (see chart 25). Given the high investment in manual review, coupled with no increase in staffing and the need to increase manual review productivity to manage increased sales with the same level of staff, more merchants cited streamlining the manual review process as their top priority for the coming year. Streamlining the tasks/ workflow occurring during the manual review process was the second ranked priority, with 21% of merchants saying it was their major focus for 2011.

The continued reliance on manual review we have seen in the data over the last few years is not an optimal long term strategy for managing online fraud. As budgets come under increasing pressure, merchants will need to redouble their efforts to automate more of the fraud management process, while keeping valid order conversion high and fraud loss low.

Resources & Solutions

To find information on CyberSource's industry-leading risk management solutions, self-paced webinars on decision management, and other whitepapers on electronic payment management, visit our Resource Center at www.cybersource.com. For sales assistance phone: 1-888-330-2300; or e-mail: sales@cybersource.com.

CyberSource Payment Management Solutions

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

Accept All Popular Payment Types in 190+ Countries

Accept payments worldwide using a merchant account from your preferred provider or CyberSource: worldwide credit and debit cards, regional cards, direct debit, bank transfers, electronic checks and alternative payment types such as Bill Me Later and PayPal. CyberSource also provides professional services to help you integrate payment with front-end and back-office systems.

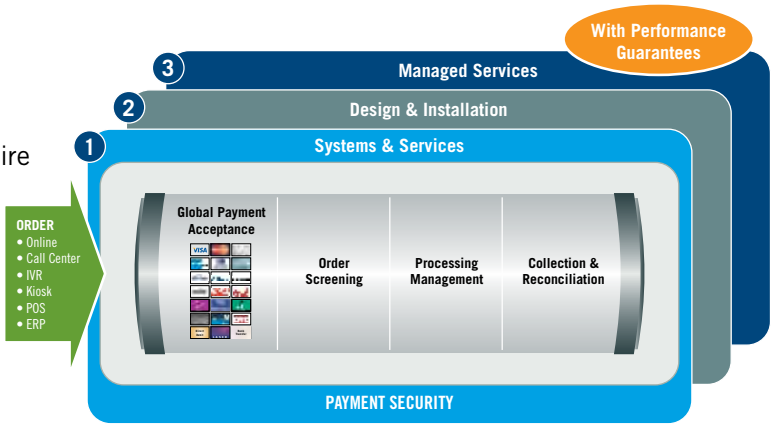
CyberSource processes your payments in our high availability datacenters located in the U.S., Europe, and Japan. All datacenters are certified PCI-compliant and include sophisticated processing management logic to help prevent payment failures and rate downgrades.

A full array of online and exportable payment reporting capability is available to streamline reconciliation activity. Depending on your merchant account provider, our reporting systems can help you automate nearly 100% of your reconciliation workflow.

Risk Management/Order Screening

Global Fraud Management Portal with CyberSource Intelligent Review Technology. A hosted rules and case management system that 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 packet signature inspection, IP geolocation, purchase velocity, identity morphing and custom data from your systems. Case management system provides consolidated data review, workflow management and built-in callouts to validation services to streamline review.

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



Payment Security

Remove Payment Data From Your Environment – Tokenization and More. A great way to streamline PCI compliance and mitigate security risk. CyberSource provides payment tokenization with remote secure storage and hosted payment acceptance services that let you capture and process payments without storing or transmitting payment data. Our outsourced screening management services can help you further eliminate staff contact with payment data.

Payment System Centralization. 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 datacenters.

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 additionally available to help you monitor, tune, or fully outsource portions of your payment operations.

North America

CyberSource Corporation HQ
1295 Charleston Road
Mountain View, CA 94043
T: +1 650 965 6000
F: +1 650 625 9145
Email: sales@cybersource.com

Europe

CyberSource Ltd.
The Waterfront
300 Thames Valley Park Drive
Thames Valley Park
Reading RG6 1PT
United Kingdom
T: +44 (0) 118 929 4840
F: +44 (0) 870 460 1931
Email: uk@cybersource.com

Japan

CyberSource Japan
3-25-18 Shibuya, Shibuya-ku
Tokyo, 150-8530 Japan
T: +81 3 5774 7733
F: +81 3 5774 7732
Email: sales@cybersource.co.jp

Asia Pacific

CYBS Singapore Pte Ltd
30 Raffles Place
#10-00 Chevron House
Singapore 048622
T: +65 6499 2000
F: +65 6437 5879
Email: asia@cybersource.com

About CyberSource

CyberSource, a wholly-owned subsidiary of Visa Inc., is a payment management company. Over 300,000 businesses worldwide use CyberSource and Authorize.Net brand solutions to process on-line payments, streamline fraud management, and simplify payment security. The company is headquartered in Mountain View, California with international offices in Reading, U.K.; Singapore; and Tokyo. CyberSource operates in Europe under agreement with Visa Europe. For more information, please visit www.cybersource.com.

For More Information

- Call **1.888.330.2300**
- Email **info@cybersource.com**
- Visit **www.cybersource.com**

Get Tailored Views of Risk Management Pipeline™ Metrics

To get a view crafted for your company's size and industry, please contact CyberSource at 1.888.330.2300 or online at www.cybersource.com/contact_us.

For additional information, whitepapers and webinars, or sales assistance:

- **Contact CyberSource: 1.888.330.2300 or www.cybersource.com/contact_us**
- **Risk Management Solutions: visit www.cybersource.com/products_and_services/risk_management/**
- **Global Payment & Security Solutions: visit www.cybersource.com/products_and_services/global_payment_services/**
- **Payment Security Solutions: visit www.cybersource.com/products_and_services/payment_security/**