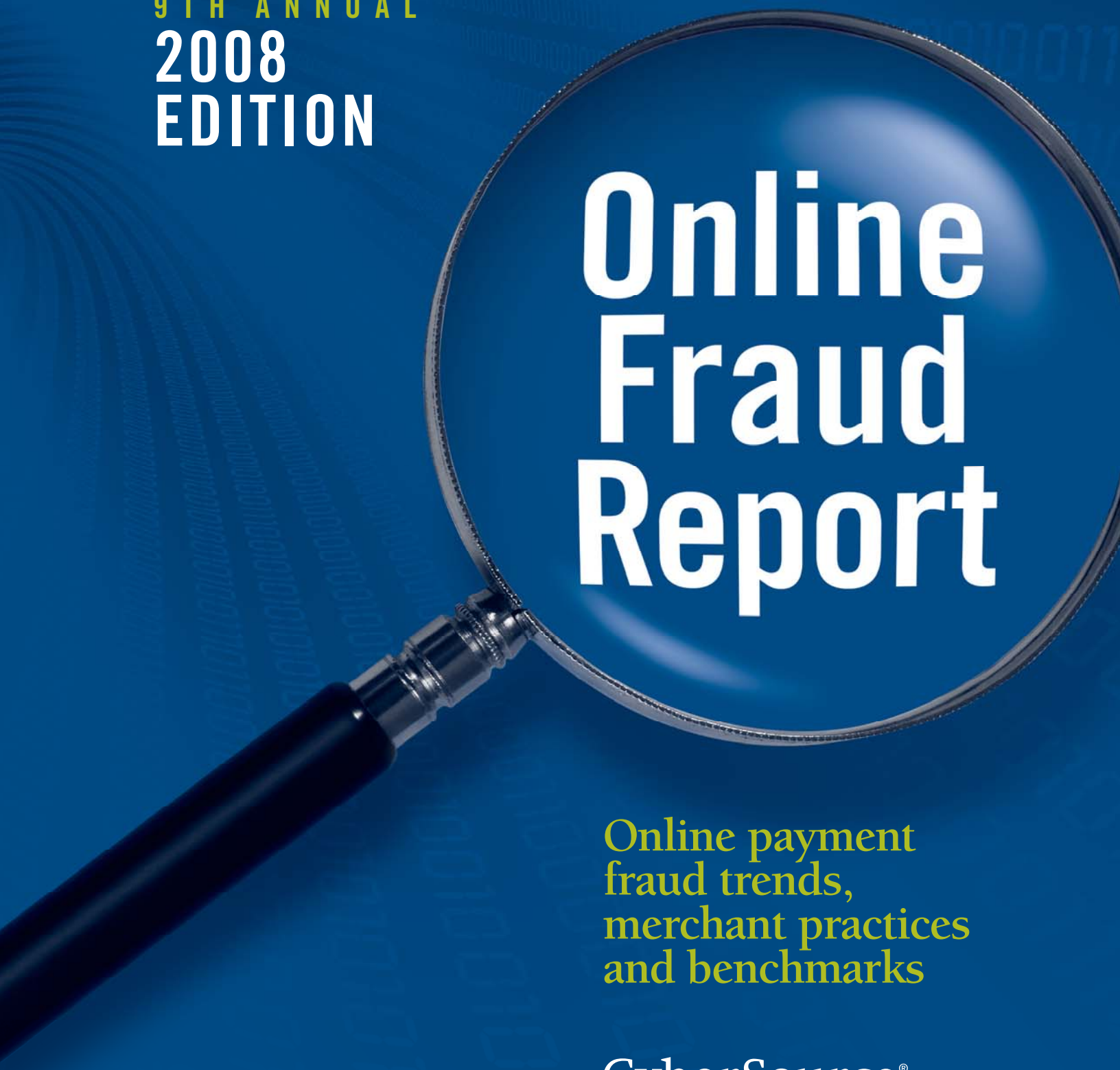
9TH ANNUAL

2008 EDITION

Online Fraud Report



Online payment fraud trends, merchant practices and benchmarks

CyberSource®

the power of payment

Report & Survey Methodology

This report is based on a survey of 318 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 the largest e-retailers and digital distribution entities in the world with many years of experience. Merchants participating in the 2007 survey reported a total estimate of $50 billion for their 2007 online sales. Survey respondents include both non-CyberSource and CyberSource merchants.

The survey was conducted via online questionnaire by Mindwave Research. Three hundred and eighteen organizations completed the survey between September 13th and October 1st, 2007. All participants were either responsible for or influenced decisions regarding risk management in their companies.

Summary of Participants Profiles

Online Fraud Survey Wave	2003	2004	2005	2006	2007
Total number of merchants participating	333	348	404	351	318
Annual Online Revenue					
Less than $500K	29%	34%	50%	37%	29%
$500K to Less than $10M	43%	39%	24%	30%	35%
Over $10M	28%	27%	26%	33%	37%
Duration of Online Selling					
Less than One Year	10%	12%	14%	11%	5%
1-2 Years	19%	14%	19%	11%	13%
3-4 Years	44%	30%	23%	18%	18%
5 or More Years	27%	44%	45%	61%	67%
Risk Management Responsibility					
Ultimately Responsible	49%	50%	60%	54%	55%
Influence Decision	51%	50%	40%	46%	45%

Get Tailored Views of Risk Management Pipeline™ Metrics

A summary of CyberSource's full pipeline process analysis is provided in the Appendix. 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/**

Table of Contents

EXECUTIVE SUMMARY **4**

STAGE 1: AUTOMATED SCREENING **6**
- Fraud Detection Tools 6
- Planned 2008 Fraud Tool Use 8
- Automated Decision/Rules Systems 9

STAGE 2: MANUAL REVIEW **10**
- Manual Order Review Rates 10
- Manual Order Review Efficiency 11
- Actions Taken During Review 11
- Final Order Disposition 12

STAGE 3: ORDER DISPOSITIONING (ACCEPT/REJECT) **13**
- Post-Review Order Acceptance Rates 13
- Overall Order Rejection Rates 14

STAGE 4: FRAUD CLAIM MANAGEMENT **15**
- Fighting Chargebacks 15
- Chargeback Management Tools 16
- Chargebacks—Only Half the Problem 16
- Fraud Rate Metrics 17

TUNING & MANAGEMENT **19**
- Maintaining and Tuning Screening Rules 19
- Global Fraud Portals 19
- Merchant Budgets for Fraud Management 19
- Budget Allocation 20

APPENDIX **22**
- Sample Risk Management Pipeline Metrics 22

RESOURCES & SOLUTIONS **23**
- CyberSource ePayment 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 ninth annual survey.

Overview

Over the past few years the percent of online revenues lost to payment fraud has been slowly declining from 1.8% in 2004 to 1.4% this year. However, total losses from online payment fraud in the U.S. and Canada have steadily increased during this time as eCommerce has continued to grow 20% or more each year.[1] In 2007, we estimate that $3.6 billion in online revenues will be lost to online fraud — up from $3.1 billion in 2006.

Key Fraud Metrics

The percent of accepted orders which are later determined to be fraudulent increased slightly. In 2007 the survey shows the overall average fraudulent order rate was 1.3% vs. 1.1% in 2006. The share of incoming orders merchants decline to accept due to suspicion of payment fraud was also up slightly. In 2007 the overall order rejection rate due to suspicion of fraud was 4.2% compared to 4.1% in 2006. Some merchants of similar online revenue size selling similar goods online have order rejection rates significantly below 4% while still maintaining low fraud rates. Therefore, we believe that merchants with order rejection rates near or above the 4.2% rate are rejecting a significant number of valid orders.

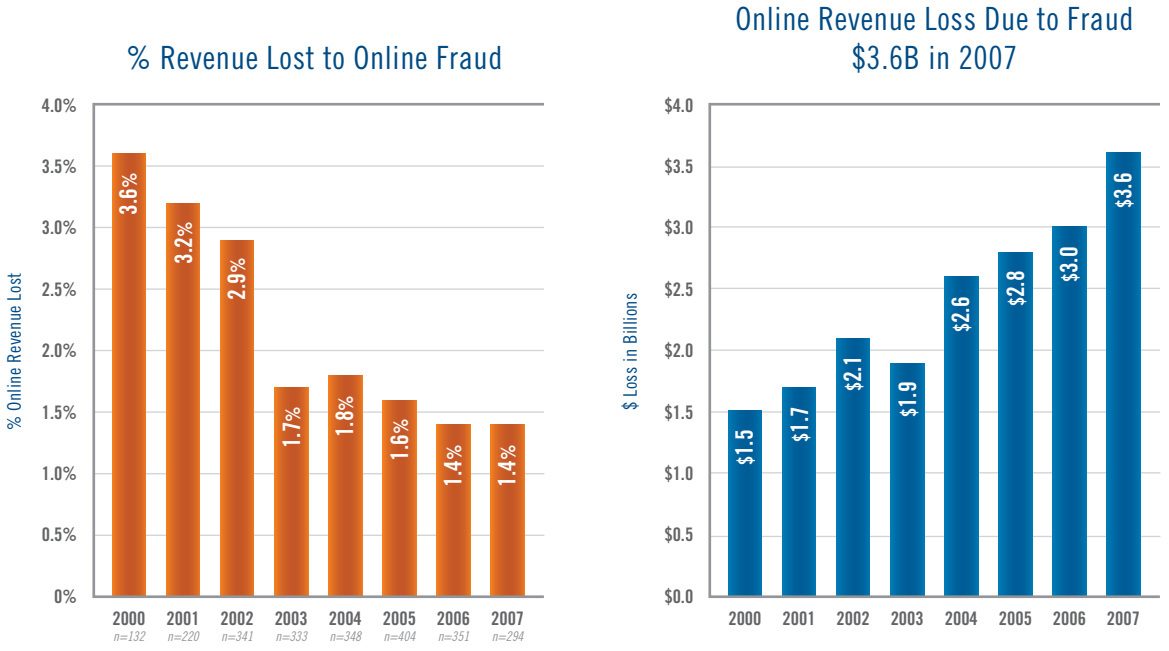
Chargebacks Understate Fraud Loss by as Much as 50%

This year's survey again probed the percent of fraud losses accounted for by chargebacks versus those incurred as a result of merchants issuing credit to reverse a charge in response to a consumer's claim of fraudulent account use. Overall, merchants continue to report that chargebacks accounted for less than half of fraud losses.

International Order Risk 2 ½ Times Higher Than Domestic Orders

On average, merchants say the rate of fraud associated with international orders is over two-and-one-half times as high as domestic orders. Merchants also reject international orders at a rate two-and-one-half times higher than domestic orders.

1



Although the rate of revenue loss due to online payment fraud has declined in 2007, total dollars lost to fraud have increased due to increased online sales growth.

[1] U.S. Census Bureau Retail E-Commerce Sales reports, Shop.org & Forrester Research.

Manual Review Rates Increase

After declining in 2006, manual review rates moved back towards levels recorded in 2004 – 2005. Manual review rates increased from an average of 23% of orders in 2006 to 27%. Overall 82% of merchants are engaging in manual order review. These merchants on average are reviewing one out of every three orders. Large online merchants, who typically employ more automation, continue to have much lower manual review rates. In 2007 large online merchants ($25+ M in online sales) reported a small drop in manual review rates from 15% to 14%. However, for many large merchants the drop in manual review rates did not offset their growth in online orders so it is likely that they are reviewing more orders. Survey data indicates that, in total, online merchants increased their spending on manual review staff in 2007 by as much as $100 million.

Efficiency Gains of As Much As 20% May Be Required

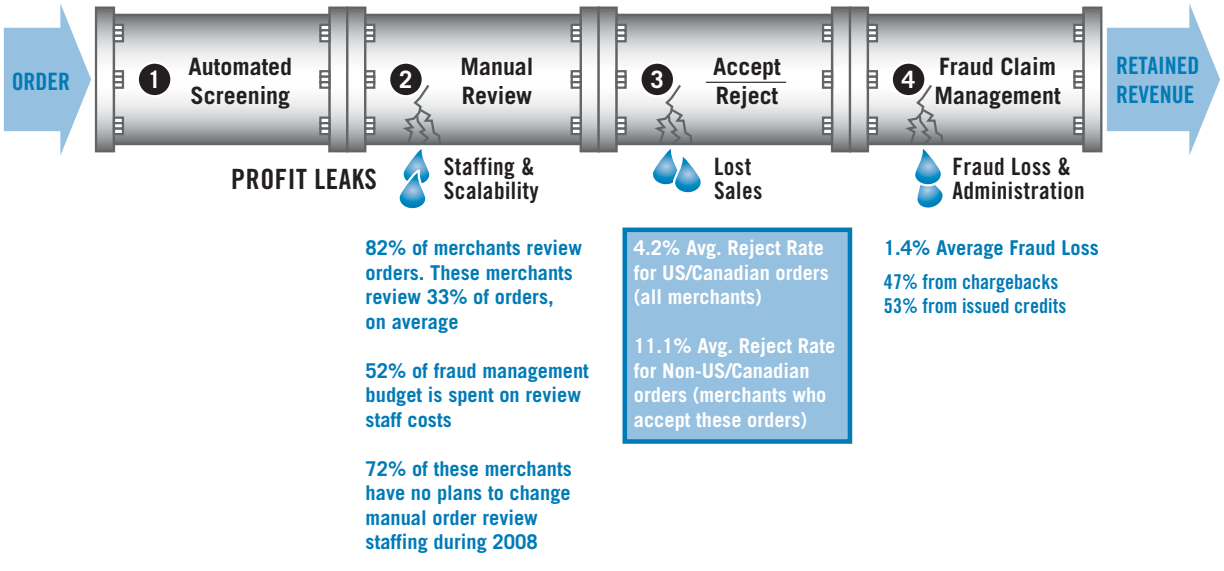
As online eCommerce sales continue to grow 15% to 20% per year, merchants face the growing problem of screening more online orders. Continued reliance on manual review presents a serious challenge to scalability. Can merchants grow their review staffing sufficiently to keep pace with fraud? Only 20% of online merchants report having budget to increase manual review staff in 2008 to cope with higher order volumes. Therefore, each year, merchants must increase fraud management efficiency approximately 20% just to keep pace.

Total Pipeline View

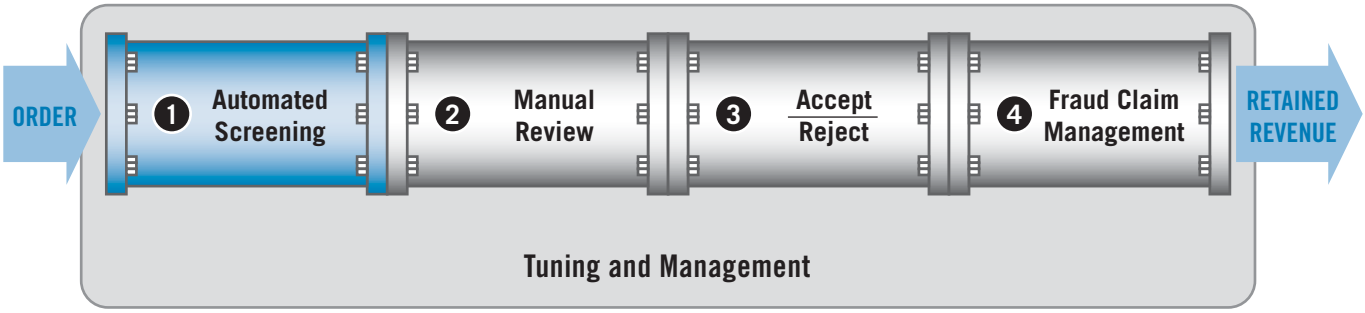
Businesses that focus solely on managing chargebacks may not be seeing the complete financial picture. Online payment fraud impacts profits from online sales in multiple ways. Besides direct revenue losses plus cost of stolen goods/services and associated delivery/fulfillment costs, there are the additional 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 association limits), an end-to-end view is required to arrive at the best possible financial outcome.

In 2007, these "profit leaks" in the Risk Management Pipeline™ impact as much as 47+% of orders for medium merchants and as much as 19+% 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, hopefully, insight. Custom views of these benchmarks and practices are available through CyberSource—see end of report for contact information.

Risk Management Pipeline



Stage 1: Automated Screening

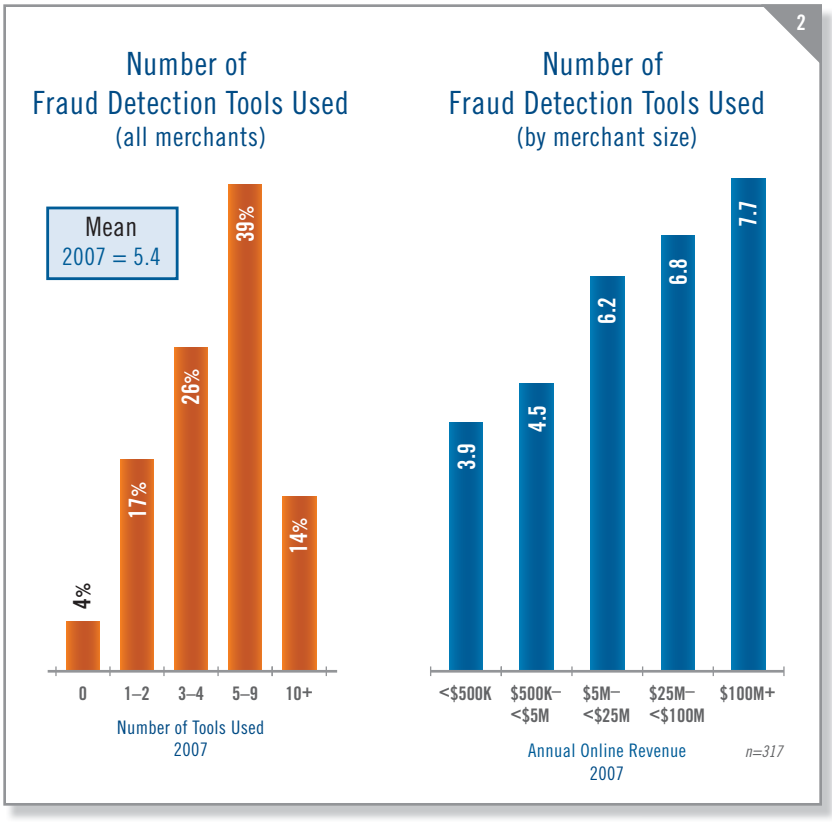


Fraud Detection Tools

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. In 2007, over three-fourths of merchants reported using three or more fraud detection tools, with 5.4 tools being the average; up from 4.8 tools on average in 2006. Larger merchants dealing with higher order volumes reported using seven 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 use more company-specific risk scoring models, negative and positive lists, and sophisticated order velocity monitoring tools.

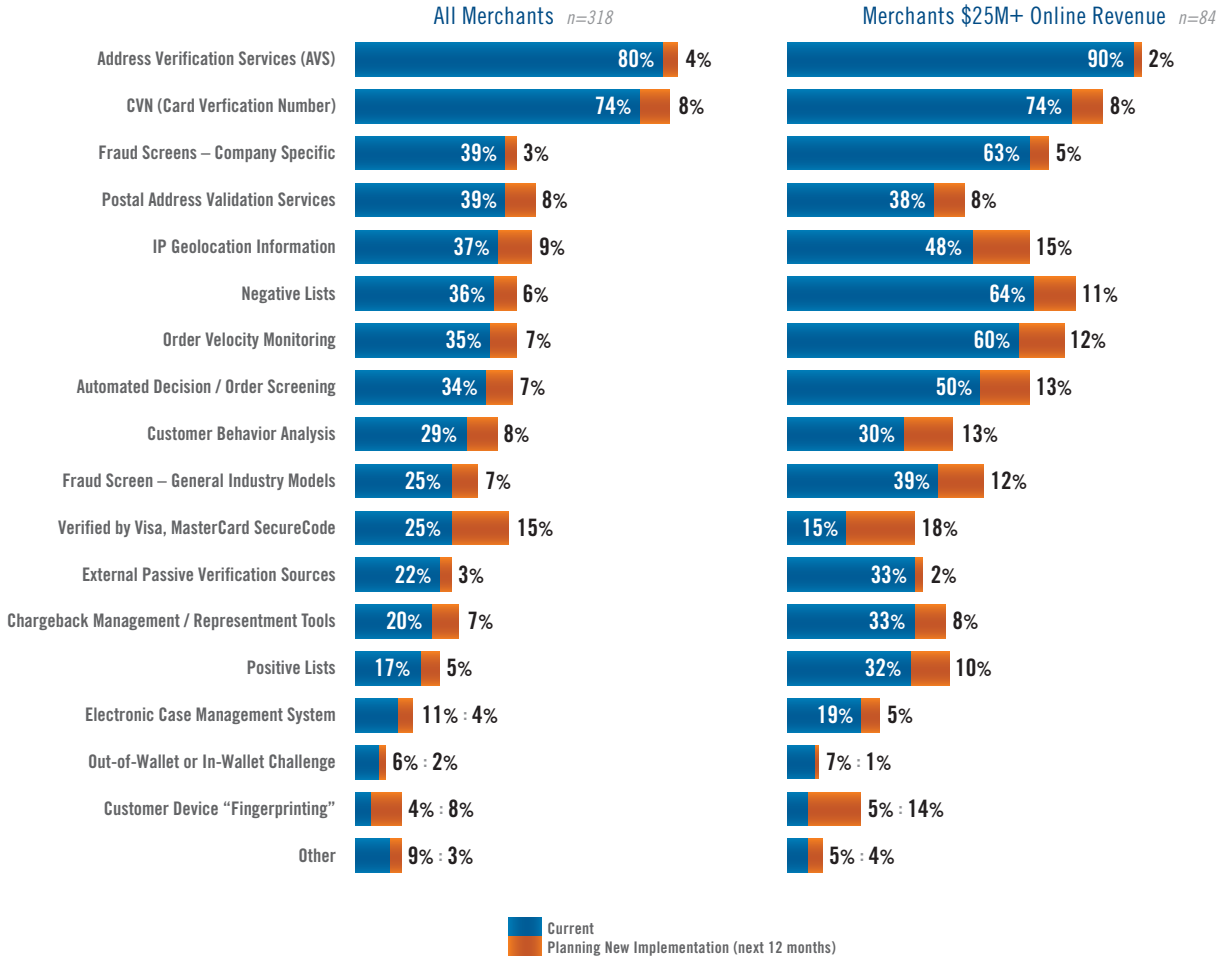
The tool most often mentioned by merchants is the Address Verification Service (AVS) which compares numeric address data with information on file from the cardholder's card issuing bank. AVS is generally available for US cardholders and for limited numbers of cardholders in Canada and the UK. AVS is subject to a significant rate of "false positives" which may lead to rejecting valid orders as well as missing fraudulent orders.[2] 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 flagged as invalid. Merchants typically do not rely solely on AVS to accept or reject an order.



[2] CyberSource analyzed 9.4 million credit card transactions where AVS was used and the final status of the transaction was known. If a merchant were to reject orders based solely on an AVS "no match" they would reject 5.7% of their orders but fail to detect 83% of the fraudulent orders. This represents an 18:1 false positive ratio.

3

Fraud Detection Tool Usage 2007



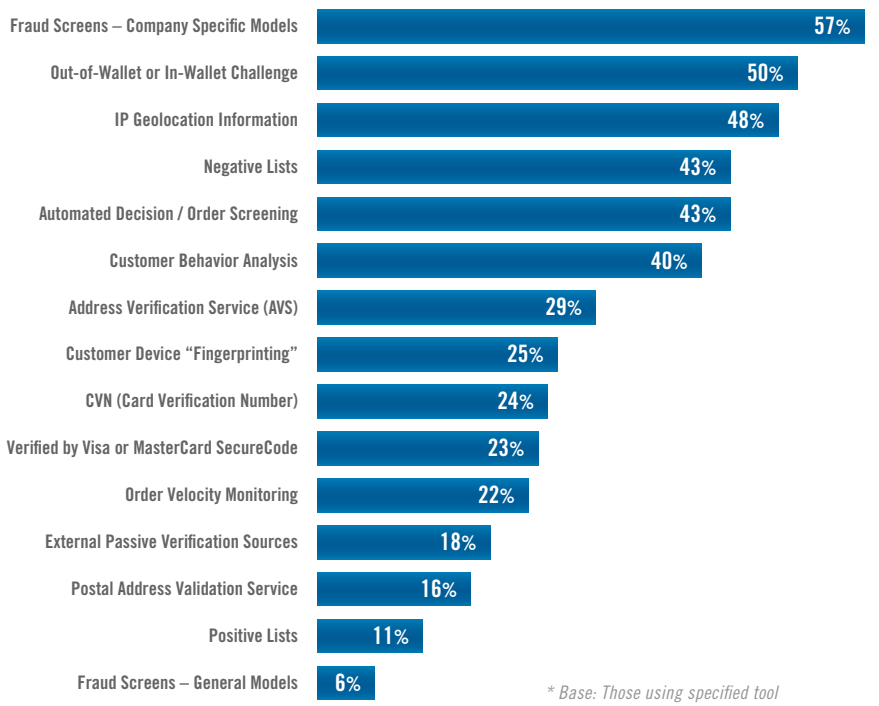
Card Verification Number (CVN; also known as CVV2 for Visa, CVC2 for MasterCard, CID for American Express and Discover) is the second most commonly used detection tool. The purpose of CVN in a card-not-present transaction is to attempt to verify that the person placing the order has the actual card in his or her possession. Requesting the card verification number during an online purchase can add a measure of security to the transaction. However, CVN numbers can be obtained by fraudsters just as credit card numbers are obtained. CVN usage by online merchants has continued to increase rising from 44% of online merchants using this tool in 2003 to 74% today.

Customer behavior analysis was added to the list this year and was cited by approximately 30% of merchants as a tool and practice they currently use. The definition provided for "Customer Behavior Analysis" was: Analyzing website traffic and flow for fraud analysis in order to profile how fraudsters navigate a website as compared to valid customers. An example of a potential fraud pattern is if a visitor to a website filled a shopping cart and went to checkout in just a few seconds which might be an indicator of an automated fraud attack. Authentic customers, even repeat customers, will typically have certain norms of behavior with respect to what pages they visit and actions they take prior to checkout and shoppers who appear outside these norms can indicate higher fraud risk.

Most fraud management tools experienced an increase in adoption in 2007. Interesting and emerging fraud tools include in/out of wallet challenges (where online buyers are asked specific personal background questions during

4

Most Effective Fraud Management Tools
% of Merchants who selected tool as one of their three most effective*



** Base: Those using specified tool*

(Merchants $25M+ Online Revenue)

the online order process) and device fingerprinting (which examines and records details about the configuration of the device the order is being placed from). Both of these are in their infancy with adoption rates of less than 10% of merchants surveyed.

In the 2007 survey we asked large merchants to identify the most effective tools they use. Merchants were asked to select, from the tools they each used, up to three tools they thought were the most effective. To eliminate the bias that the more commonly used tools have the potential to receive more mentions, we normalize the data by looking at what percent of merchants using a particular tool cite that tool as one of their top three choices. Chart #4 shows the results of this analysis.

Company specific fraud screens received the highest rating as being an effective tool by merchants who use this tool. 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 we typically find that most risk scoring models need regular tuning with new analysis and data in order to maximize their effectiveness.

Out-of-wallet or in-wallet challenge systems, while used by only 7% of large merchants today, was rated by half of these merchants as being one of their three most effective tools.

Planned 2008 Fraud Tool Use

Payer Authentication Services Cited As Tool Most Often Planned For Implementation in 2008

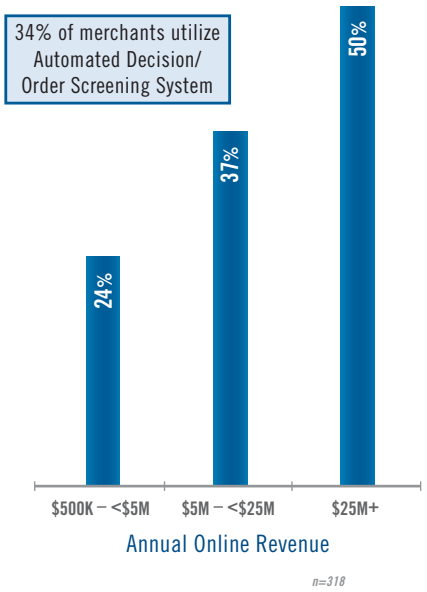
Card association payer authentication services (e.g. Verified by Visa, MasterCard SecureCode) figure prominently in many merchants' future plans. 2007 survey results show that one out of four merchants currently use one or more of the available payer authentication services. Similar to last year's survey, 15% of respondents say they are interested in deploying these systems in the next twelve months as a new tool to manage fraud. However, despite significant interest in implementing payer authentication systems over the past few years, we have seen relatively slow actual adoption of payer authentication since we started tracking this tool in 2003. In that year, one out of five online merchants reported using payer authentication. Implementing these systems 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 association may not permit the merchant to shift liability even if the merchant has implemented a payer authentication system. Over the next few years, 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. Merchants will still need to have procedures in place to handle customers who have not adopted the new systems or who use cards which are not yet supported. The growing

popularity of online payment types such as electronic checks, PayPal, Bill Me Later, etc. will also require different fraud management techniques.

After payer authentication systems, IP geolocation tools are the second most popular tool for planned implementation in 2008. IP geolocation attempts 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.

5

Automated Decision / Order Screening System Utilization
(by merchant size)



Automated Decision/Rules Systems

Automated Order Screening

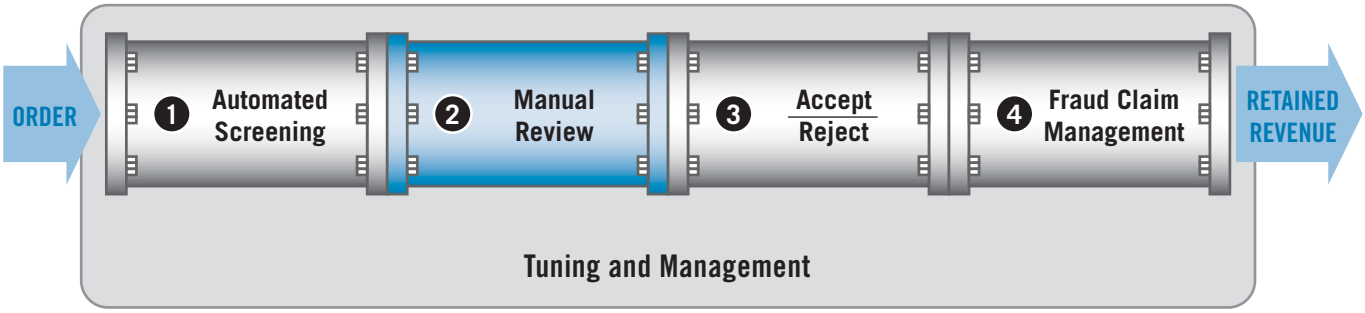
Automated order decisioning / screening is now used by 34% of merchants (up from 25% in 2005). Half of the larger online merchants use them. These tools help companies automate order screening by applying a merchant's business rules in the real-time evaluation of incoming orders. In the current survey, 7% of merchants say they plan to add this capability in 2008. 13% of larger merchants (more than $25 million in annual online revenues) say they will add order decisioning systems, consistent with their need for increased automation.

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 use of tools 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. Because fraud patterns are dynamic, and the introduction of new products or services often requires a unique set of acceptance rules, it is imperative that these systems can also quickly adapt to the changing environment.

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. In our experience, most merchants avoid automatic rejection of orders and instead send all orders marked for review or reject into a manual review queue for further validation.

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 collected about the order to determine if it 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 impacts customer satisfaction. Few merchants say they have budget available to increase review staff now or in the next twelve months. This situation presents significant challenges to profit growth since, even at a stable percent of orders sent to review, the total number of orders that must be reviewed increases in step with the total increase of online sales.

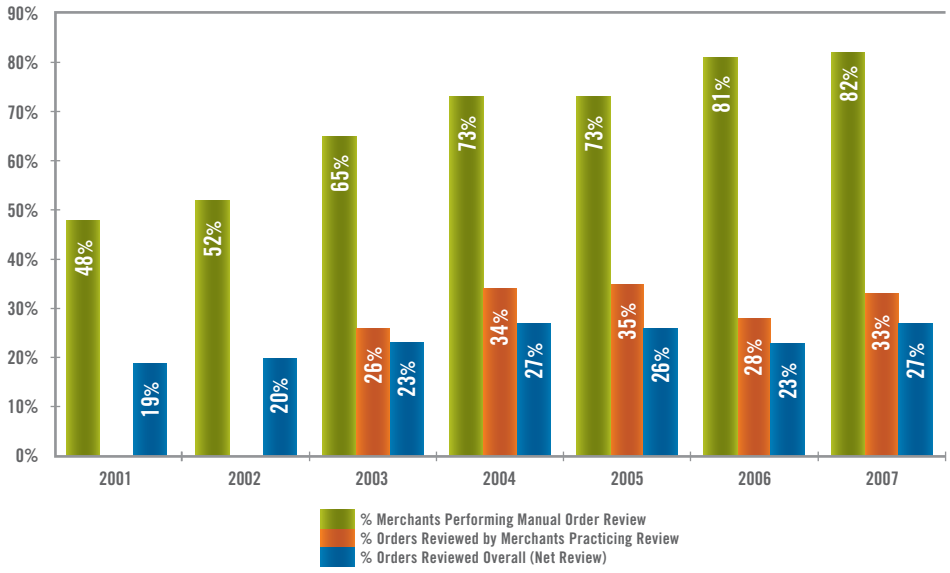
Manual Order Review Rates

In what should be a highly automated sales environment, 82% of merchants are manually checking orders today. The average rate of manual review for these merchants is 1 out of 3 orders. Projecting this rate across all merchants and orders, approximately 27% of all online orders (about one in four) were reviewed in 2007, as compared to 19% in 2001 (approximately one in five orders).

Merchants of all sizes use manual review to manage payment fraud. Chart #7 (see page 10) shows smaller merchants review a higher percentage of orders (perhaps because lower order volumes permit such practice) but

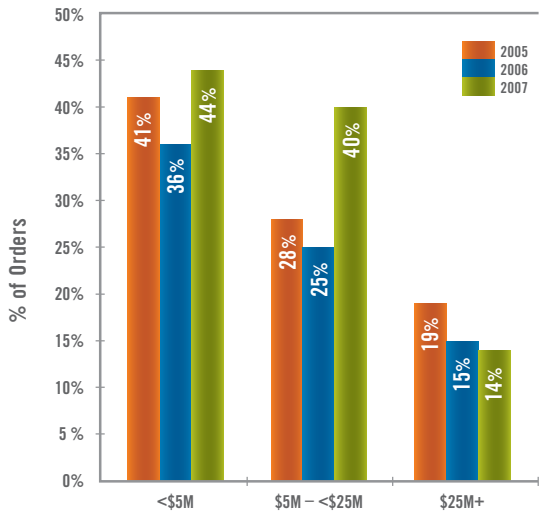
6

Manual Review Trends



7

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



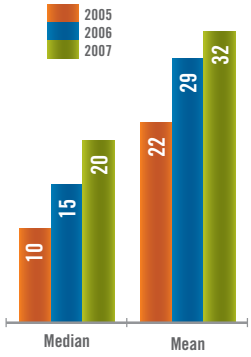
8

Orders Reviewed Per Hour/Reviewer
(by review rate)
2007

# Orders	% of Merchants
<10	24%
10–19	24%
20–49	28%
50+	24%

n=148

Orders Reviewed Per Hour/Reviewer



even larger merchants review a significant percentage of online orders—and likely devote more resources to this task than is operationally scalable.

It appears from the 2007 survey results that small and medium size online merchants significantly increased the percent of orders they manually reviewed while large merchants reported a small decrease. Across all merchant sizes manual review rates for merchants engaging in review increased from 28% in 2006 to 33% in 2007 or an 18% increase in the average rate. Considering that overall internet sales growth in 2007 was approximately 20% this implies that many merchants saw a 30 – 40% increase in the number of orders they manually reviewed in 2007. Even large merchants probably saw some increase in the total number of manually reviewed orders. It may be that one consequence of using more fraud detection tools is that there is a greater chance of one or more flags being raised resulting in an order being selected for manual review. Adding additional 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.

Given that double digit online sales growth will likely continue for the foreseeable future, merchants who manually review significant portions of orders 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 their methods of identifying riskier orders for review and make the review process itself more efficient.

Manual Order Review Efficiency

Given the reported limitations on hiring additional manual review staff, we have seen a concurrent and steady rise in the number of orders review staff are processing per hour. In 2007, the average number of orders a reviewer processed in an hour increased 10% from 29 per hour in 2006 to 32 per hour in 2007. In most cases, reviewers are prioritizing their time and spending more time trying to verify a few orders that look highly suspicious and spending less time on the remaining orders. As we discuss in the next section, we have seen an increase in the percentage of manually reviewed orders that are accepted which may be a forced consequence of putting more orders into the manual review process without additional staff or automation.

Actions Taken During Review

Beyond reviewing data associated with the order, additional review cycles are spent contacting various parties to validate information—causing drag on review efficiency and, perhaps most importantly, inconveniencing customers by making them wait. It appears most merchants are doing a good job of clearing orders through manual review. Two-thirds of merchants reported clearing orders in one business day or less (see chart #9). We also asked large merchants about their policy on how long they will suspend an order while waiting for a customer to confirm the order is valid. While there is a wide range of policies from less than one business day to over six business days it appears that the typical time delay allowed for customers to validate orders is 2–3 business days (see chart #10).

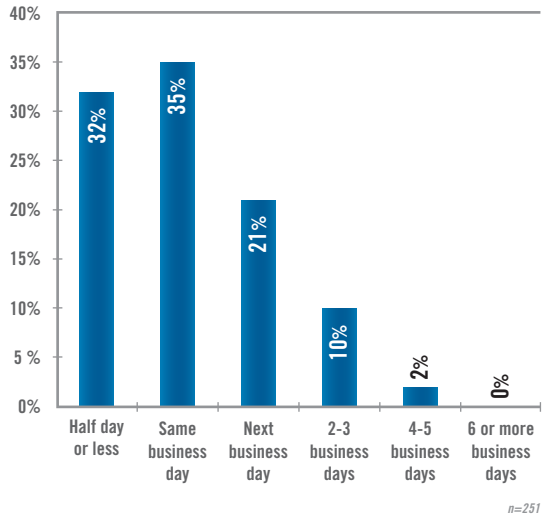
In our 2005 survey, merchants reported that 44% of orders reviewed required contacting the customer, 29% required contacting the customer's bank, and 18% of the orders required contacting third party data sources such as credit bureaus. Note that a single order may require more than one of these actions. Finding ways to eliminate these actions or to automate review processes offer great potential for enhancing profitability and scalability.

Final Order Disposition

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

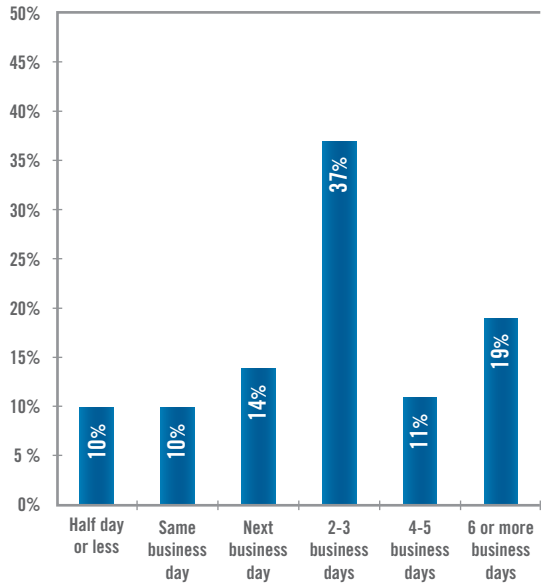
9

Time to Clear Orders in Manual Review

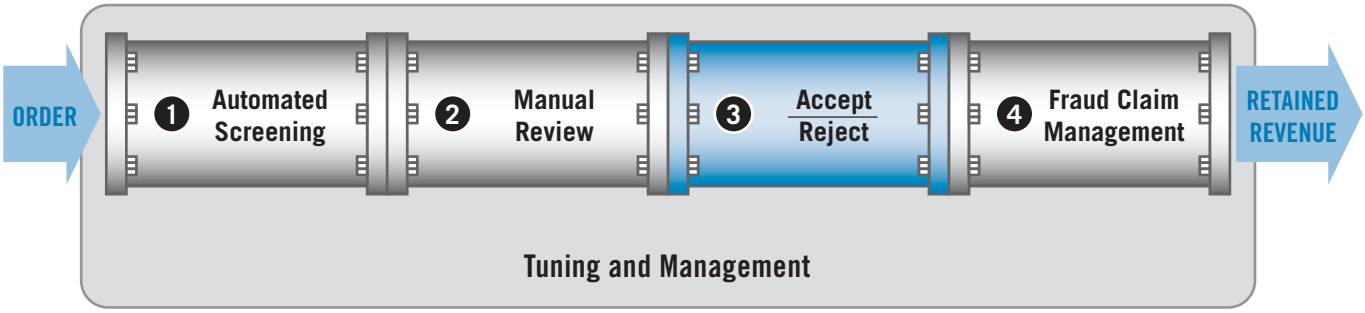


10

Time Allowed for Customer Response



Stage 3: Order Dispositioning (Accept/Reject)

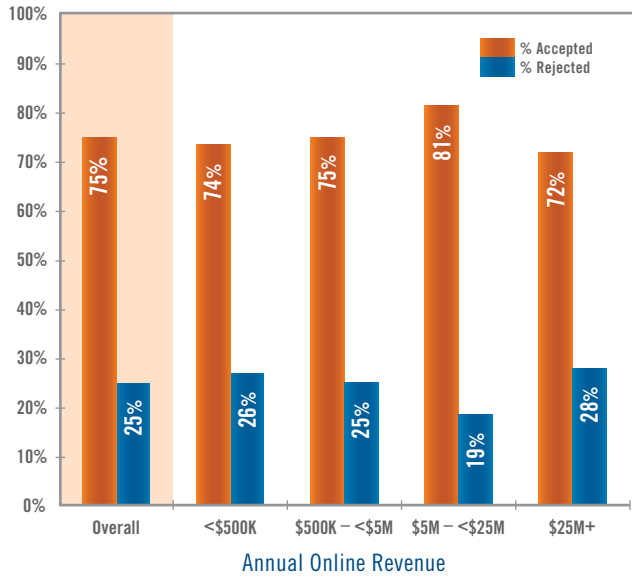


Post-Review Order Acceptance Rates

In 2007, merchants surveyed indicated that they ultimately accepted over three-fourths of the orders they manually reviewed (see chart #11). This was a noticeable increase over the two-thirds of manually reviewed orders accepted we have recorded in past surveys. Over 50% of merchants report they accept 90% or more of 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 there is a need among most merchants for better methods to out sort only the orders with high fraud risk for further manual review. It may be that the higher share of orders going into manual review in 2007 was one of the factors contributing to higher post manual review order approval rates. Reviewers, faced with 30 – 40% more orders to review, simply had to approve a higher proportion of orders overall to manage the higher volumes and concentrate their efforts on those orders they perceived as more risky.

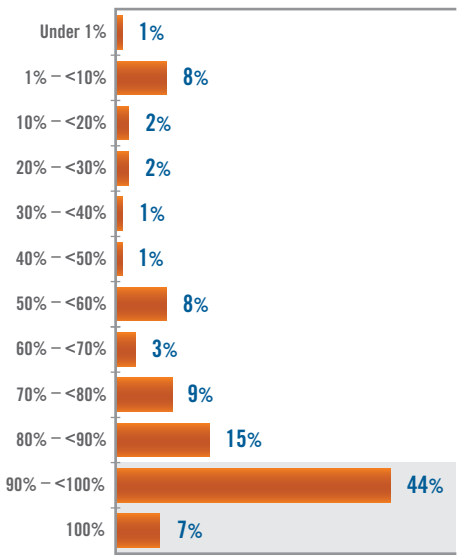
11

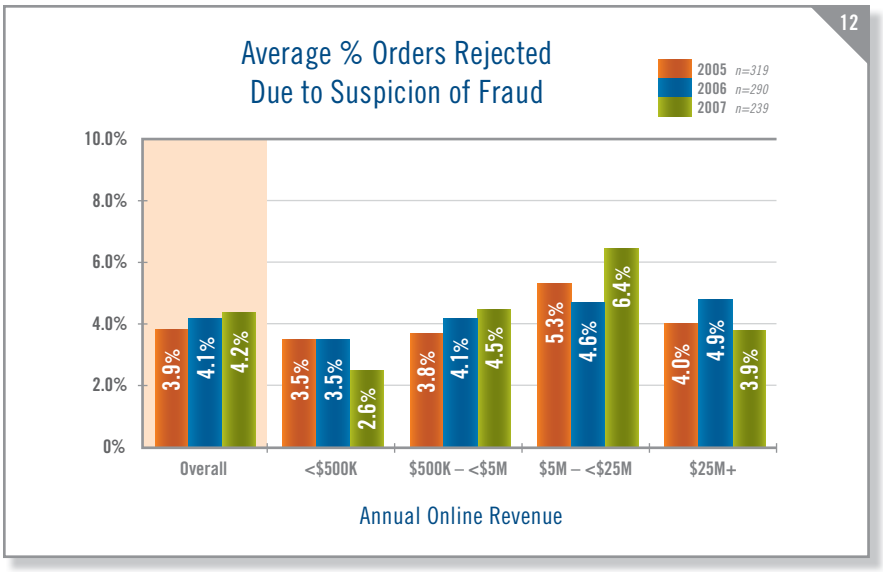
Average % of Manually Reviewed Orders that are Accepted/Rejected



n=262

% of Merchants Reporting this Level of Acceptance





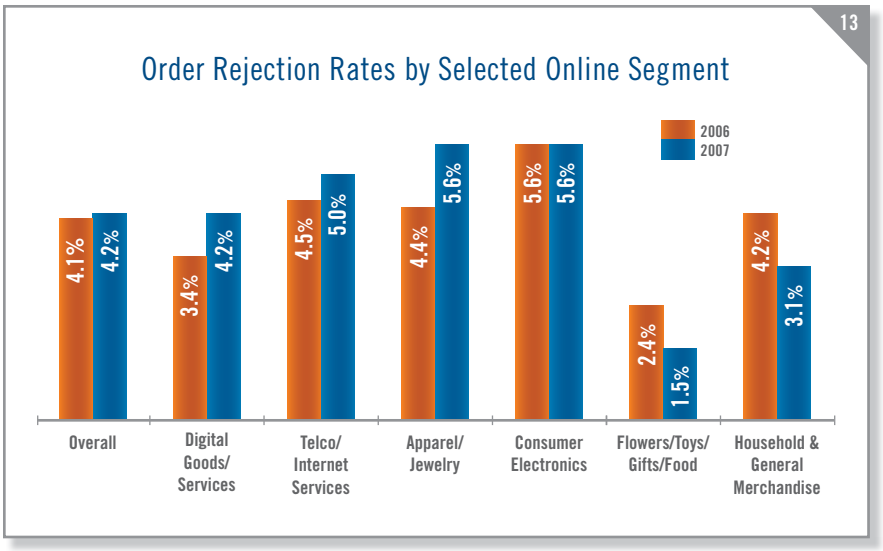
Overall Order Rejection Rates

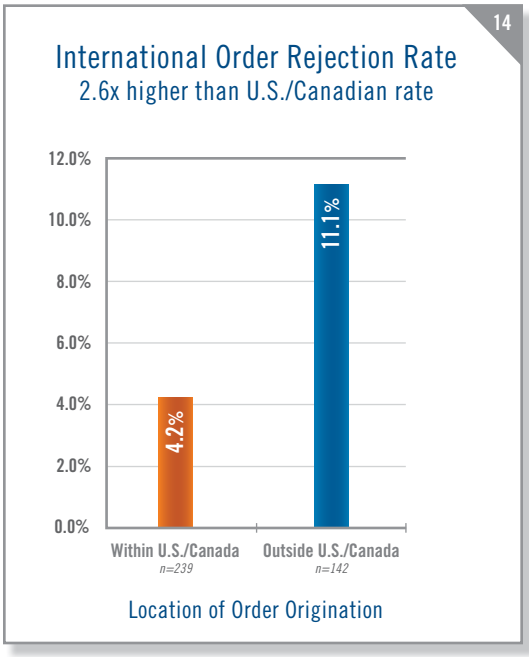
Order reject rates can reflect true fraud risk or signal "profit leaks" in terms of valid order rejection or unnecessarily high rates of manual review. In 2007, merchants participating in the survey reported a slight increase in their order rejection rates from 4.1% in 2006 to 4.2%. As chart #12 shows, the overall average order rejection rate has been trending up over the past three years from 3.9% in 2005 to the current 4.2%. In 2007, for every fraudulent order they received, merchants rejected over 3 orders due to suspicion of fraud.

Order rejection rates also vary by type of products and online merchant. Chart #13 shows that segments which are more likely to be targets for fraud and which may have high cost of goods sold and/or lower gross margins, tend to have higher order rejection rates. In these cases, of course, each fraud loss 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.

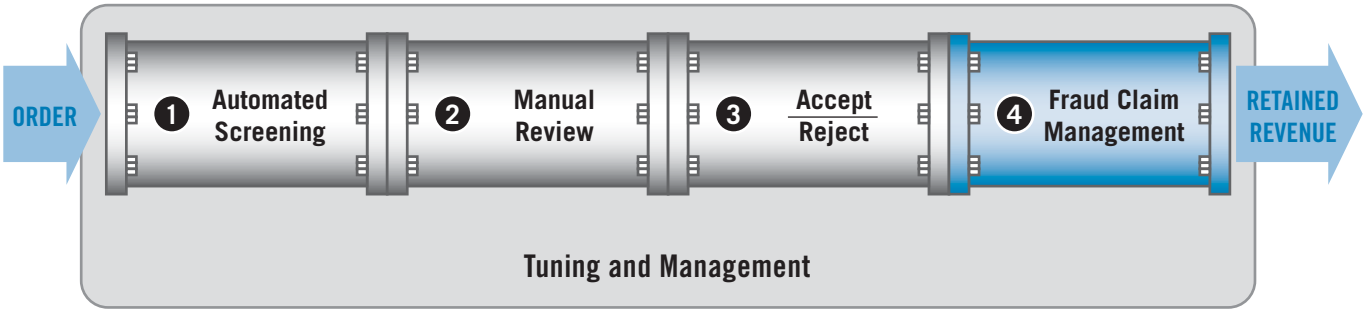
Yet, even within similar groups of online merchants we see that some merchants achieve low order rejection rates while still keeping fraudulent order rates under control. Examining the large consumer electronics merchants in the sample we find that half of these merchants report order rejection rates of 2% or less while maintaining fraudulent order rates at the average for their segment.

Merchants who accept orders from outside of North America consistently report a much higher level of order rejection due to suspicion of payment fraud for international orders. In 2007, merchants report their rejection rate on these orders is over two and one half times that of domestic orders as shown in chart #14 below. The actual fraud rate experienced on international orders supports this cautious approach as merchants report the fraud risk on international orders is also over two and one half times that of domestic orders.





Stage 4: Fraud Claim Management



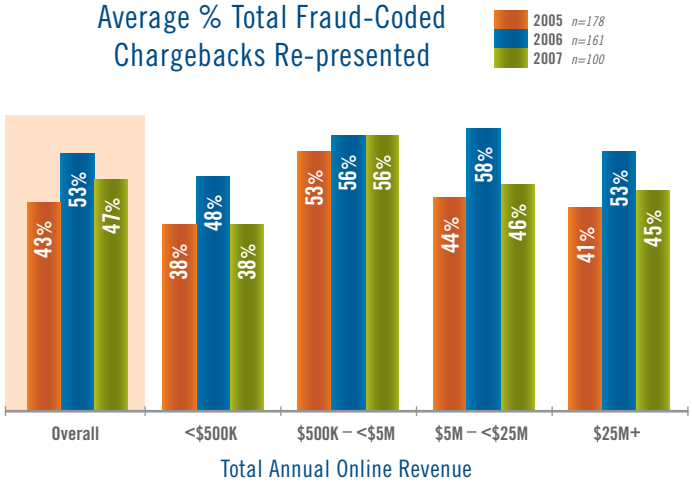
Fighting Chargebacks

This year's survey once again examined online merchants' practices associated with reviewing and contesting chargebacks ("re-presentment"). Over the past three years the share of fraud-coded chargebacks merchants contest has averaged 43% to 53%. Medium and large merchants report contesting around 45% of fraud-coded chargebacks in 2007. However, when we look at the distribution of merchants' answers to this question we find that over one third of merchants are disputing 90% or more of their fraud chagebacks while one out of four merchants are disputing less than 10% of their fraud chargebacks.

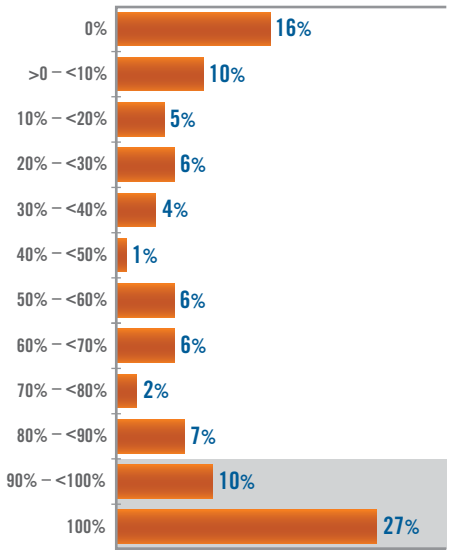
In 2007, merchants report that they win, on average, 40% of the chargebacks they dispute which is very similar to the 42% win rate they reported in 2006. Simply using the average percent of chargebacks that are disputed times the average win rate results in a net recovery rate of 19% (meaning 19% of all fraud-coded chargebacks are recovered). However, given the wide disparity in the chargeback re-presentment rate, when these are calculated

15

Average % Total Fraud-Coded Chargebacks Re-presented

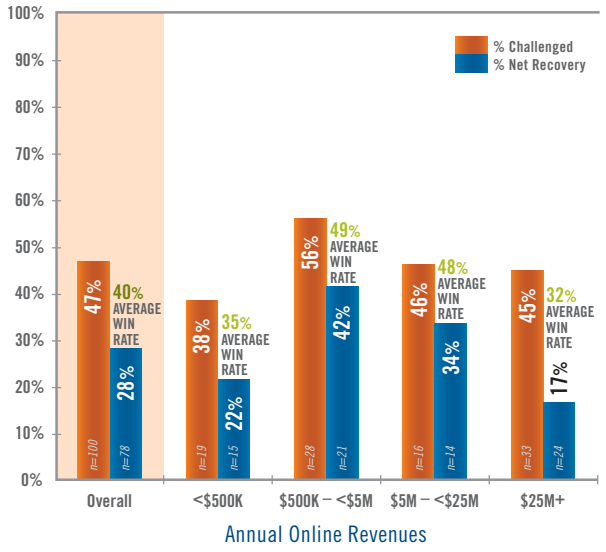


% of Merchants Reporting this Level of Re-presentment



16

Fraud Chargeback Re-presentment:
Win Rate/Net Recovery Rate
(overall and by merchant size)



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

on a merchant-by-merchant basis and then averaged, the re-presentment win rate rises to 28% (see chart #16). In 2006 this weighted net recovery rate was 32%. Therefore, disputing most fraud chargebacks and having an efficient re-presentment process can help enhance profitability and reduce fraud loss.

Chargeback Management Tools

Of course disputing chargebacks is not an easy or cost-free process. Merchants must manage and organize all order, delivery and payment information to successfully dispute fraudulent orders with financial institutions. Merchants are beginning to adopt automated systems for handling this aspect of the pipeline. One out of five merchants reported using chargeback management tools in 2007 and one out of three large merchants reported using these tools. In our 2006 survey 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 1.0 hours 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. Given the time involved plus fees and penalties, it sometimes makes economic sense for merchants to avoid chargebacks by encouraging customers to contact them directly instead of first contacting their payment provider / biller.

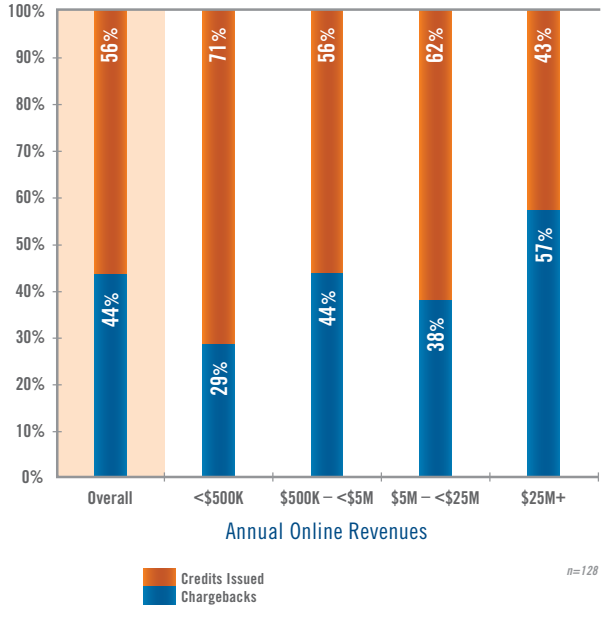
Chargebacks—Only Half the Problem

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. This is true for most sizes of merchants (see chart #17 below).

In 2006 large ($25M+ online sales) merchants reported that 47% of their fraud was presented in the form of a fraud-coded chargeback however in 2007 this has risen to 57%. 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 merchants control to either handle the dispute directly with the consumer or to advise them to initiate

17

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



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/reversal.

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 that 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 associations which generally base reported rates on chargeback activity only.

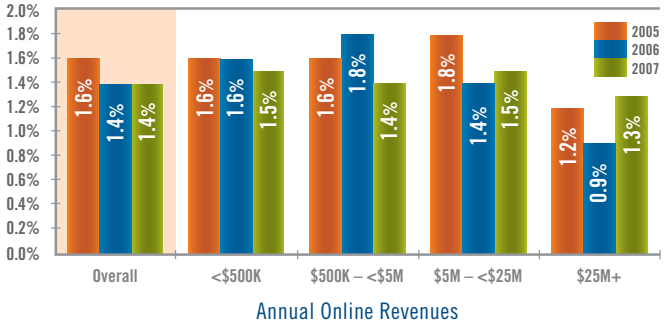
Depending on what products or services are being sold online, fraud loss risk tolerances and order rejection rates can vary significantly. Merchants selling high cost goods with relatively low gross margins, like most consumer electronics products, tend to err on the side of rejecting more orders to avoid expensive fraud losses while merchants who are less subject to fraud attacks can achieve similar fraud loss rates while rejecting relatively few orders (see Flowers/Toys/Gifts & Food merchants in chart #13). Over the past few years, as fraud rates have remained relatively stable, we have compiled data on fraud practices and benchmarks by industry (see appendix for how to obtain these benchmarks).

Direct Revenue Loss Rates

Very large merchants typically use more tools and have more experience and resources to manage online fraud so their overall fraud rates tend to be lower than the average (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. Figures include both chargebacks and credits issued directly by the merchant in response to fraud claims.

18

Average % Online Revenue Lost to Payment Fraud
(Chargebacks & Fraud-Related Credits)

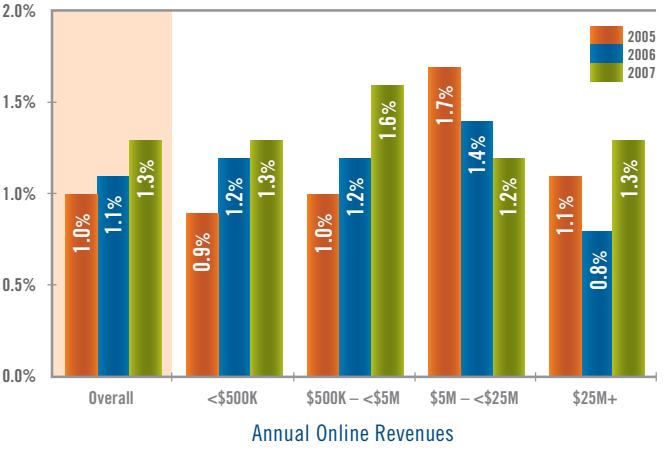


Fraudulent Order Rate for Accepted Orders

Another key metric is the number of accepted orders that later turn out to be fraudulent. Expressed as a percent of total orders, this metric is typically lower than the revenue loss percent since the average value of fraudulent orders tends to be greater than the average

19

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

value of valid orders, which causes the fraud rate as measured by revenues to be higher. Overall, 39% of merchants reported experiencing a fraudulent order rate of 1% or more in both 2005 and 2006 survey data and in 2007 it was nearly the same with 38% of merchants reporting a fraudulent order rate of 1% or more.

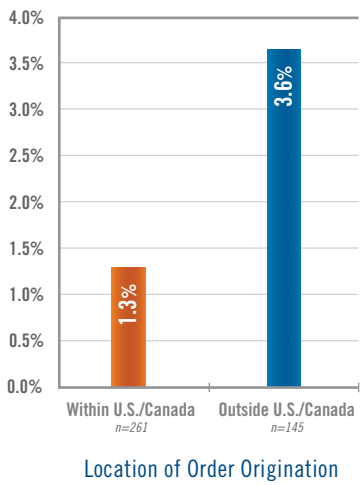
International Orders Carry Higher Risk

Fifty-nine percent of merchants surveyed accepted orders from outside the U.S. & Canada in 2007. International sales accounted for an average of 16% of total orders for these merchants. That same group reported that the actual direct fraud rate on international orders averaged 3.6%, or more than 2.7 times the overall fraud rate for domestic online orders. While online sales in the U.S. are still growing by 15 - 20% annually, sales in Europe and many other markets are showing even higher growth.

Though international markets represent an attractive opportunity, online merchants must make sure that their fraud detection and management systems are robust enough to handle the additional risk involved.

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 over two and one half times the U.S. and Canadian average rate of 4.2% — rejecting approximately 1 out of every 9 international orders received.

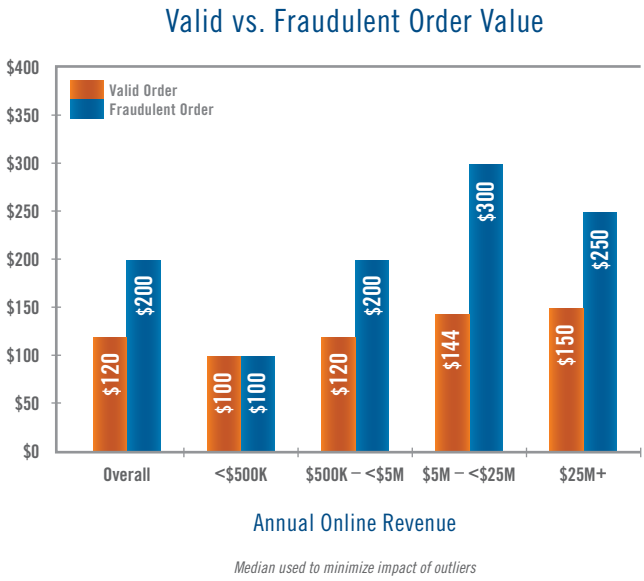
20



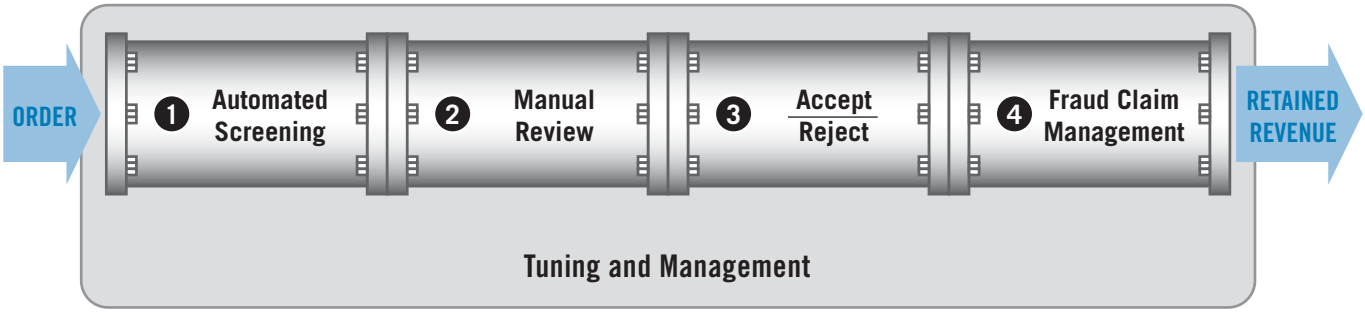
Average Value of Fraudulent Order Higher than a Valid Order

Historically fraudulent orders tend to have higher values on average than valid orders. In 2007, the median value of a fraudulent order was $200 compared to $120 median value reported for valid orders. This relationship of higher fraudulent order values vs. valid order value was found for all merchant size categories except for the smallest online merchants as chart #21 shows. Since fraudulent orders tend to be somewhat higher in value than valid orders, merchants will tend to out sort more high value orders for manual review and verification. In 2007 large online merchants reported that the median value of an order flagged for manual review was $275 as compared to $250 median value for fraudulent orders overall.

21



Tuning & Management



Maintaining and Tuning Screening Rules

Our 2006 survey indicated that, among merchants who had an automated order screening system in place, 49% had systems that allowed business managers to modify decision rules without assistance from internal IT staff or external third parties (meaning overall, only 16% of all merchants had systems in place that allow business managers to modify rules). 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 typically include hierarchical management, as companies strive to centralize fraud management across multiple lines of business and geographies.

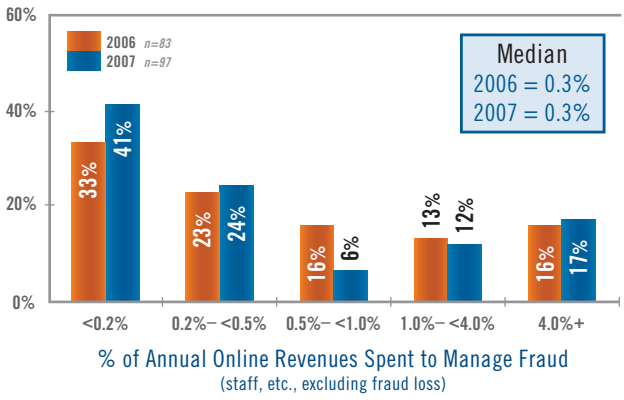
Merchant Budgets for Fraud Management

How much are online merchants spending to mitigate fraud risk? Thirty-five percent of merchants spend 0.5% or more of their online revenues to manage online payment fraud while 65% spend less than 0.5%. Again in 2007, across all merchants, the median ratio of fraud management expense to sales was 0.3%, although some merchants in high risk categories are spending significantly more. These spending estimates include the costs of mitigating 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).

22

How Much Merchants Spend on Fraud Management

(percent of merchants operating at defined expense level)



Overall, applying the median ratio of the percent of online revenues spent to manage fraud to 2007 online sales we can estimate that approximately $780 million is being spent to manage online fraud in 2007 over and above the actual fraud losses (see chart #24).

Review Staffing – 2007

# Full-Time Review Staff	Median* Annual Online Revenue	Annual Revenue per Staff
1	$775K	$775K
2	$6 Mil	$3M
3 – 4	$20 Mil	$5M – $7M
5 – 9	$60 Mil	$7M – $12M
10+	$300 Mil	up to $30M

*Median used to minimize impact of outliers

Planned Staffing Levels for 2008

Increase	Same	Decrease
20%	72%	8%

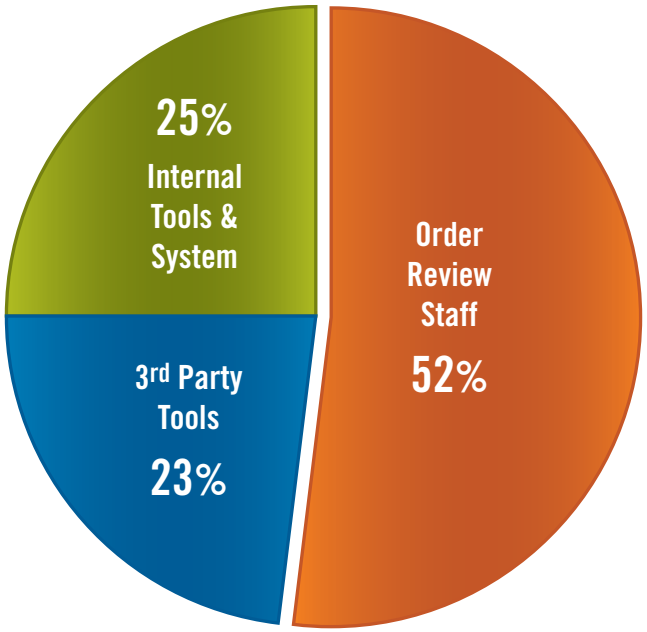
Base: Those with 1 or more full-time manual review staff

n = 248

23

Average % Spending Allocation for Fraud Management 2007

Mean (including 0)



n=318

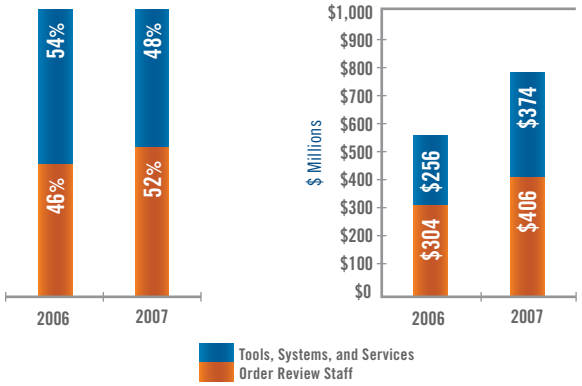
Budget Allocation

Perhaps driven by higher order review rates in 2007, the survey results show an increase in the percent of fraud management budgets spent on order review staff. In last year's survey, 46% of merchants' budgets, on average, were spent on order review staff and this has increased to 52% reported in 2007 (see chart #23). The remainder is allocated as follows: 23% for third party tools or services and 25% on internally developed tools and systems.

Clearly, review staff costs are the dominant factor, and only 20% of merchants cite plans to increase review staffing in 2007. 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 in order to reduce order review volumes.

24

Merchant Allocation of Fraud Management Spending



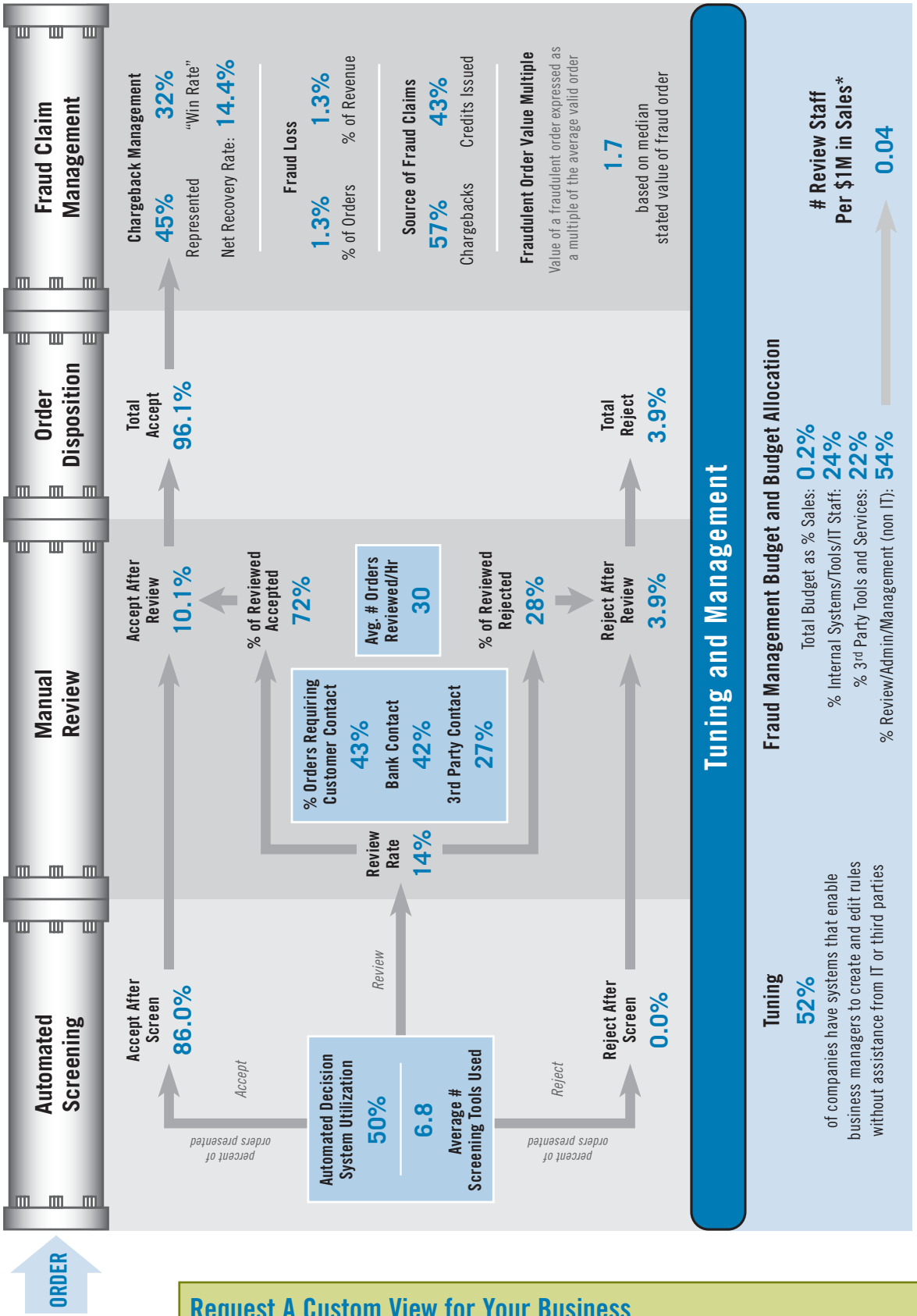
Total spent on fraud management increased 18% in 2007 in line with online sales growth

However merchants increased spending on manual review staff by 34% due to the higher volume of orders being sent to manual review

Combining our estimate of how much merchants are spending to manage fraud in 2006 and 2007 with how merchants allocated this spending, we can estimate that in 2007 merchants' spending on manual review staff increased significantly over 2006, perhaps by as much as 34% or over $100 million (see chart #24).

Clearly the increased reliance on manual review we see in the data for 2007, is not a viable long term strategy for managing online fraud. As online sales continue to grow merchants will need to redouble their efforts to automate more of the fraud management process and improve their ability to assess order risk in order to avoid even higher levels of manual order review costs.

APPENDIX: Sample Risk Management Pipeline Metrics $25+M



* data calculated based on responses to other points in the pipeline; all other data is that reported by merchant.

Request A Custom View for Your Business

This is an example of a full pipeline process analysis for select merchants in the survey. To get a view crafted for your company's size and/or industry, please contact CyberSource at 1.888.330.2300, or online at www.cybersource.com/contact_us

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 ePayment Management Solutions

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

Payment Acceptance 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.

Risk Management/Order Screening

Fraud Management Portal. A hosted rules and case management system that interfaces with over 100 validation tests and services including: multi-merchant transaction history checks, worldwide delivery address and phone verification, IP geolocation, purchase velocity, identity morphing and custom data from your systems.

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, order review and chargeback management. Our managed services include business performance guarantees.

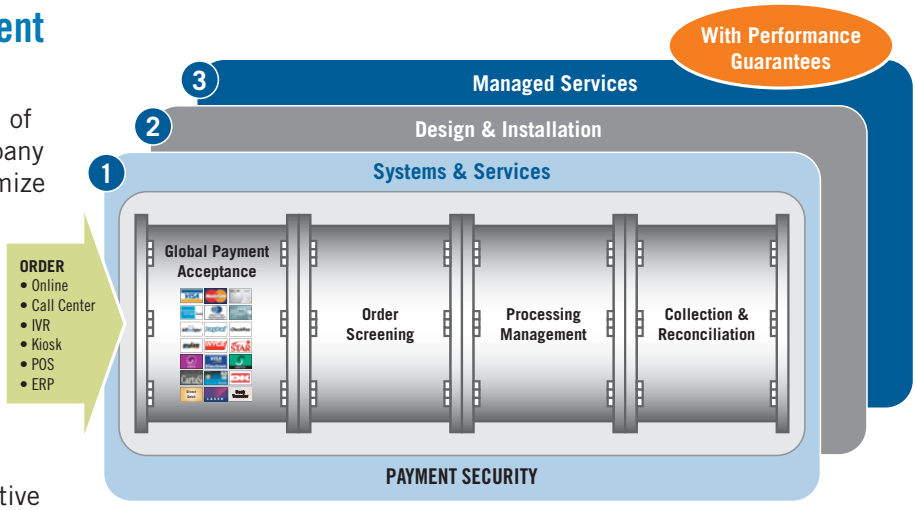
Payer Authentication. Verified by Visa, MasterCard SecureCode

Processing Management

CyberSource processes your payments in our highly 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.

Collection & Reconciliation

A full array of online and exportable payment reporting capability is available to streamline reconciliation activity. Further, systems can be installed to automate up to 90% of the tasks associated with payment reconciliation and chargeback re-presentment.



Payment Security

Remove Payment Data From Your Network. CyberSource provides secure storage and hosted payment acceptance services that let you process without storing or even transmitting payment data. A great way to streamline PCI compliance and mitigate security risk.

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

PCI Planning & Remediation. CyberSource provides PCI compliance consulting and remediation services, as well as complimentary PCI vulnerability scanning services to help you maintain compliance.

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.

About CyberSource

CyberSource Corporation is a leading provider of electronic payment, risk and security management solutions. CyberSource provides payment management solutions for electronic payments processed via Web, call center, kiosk, mobile and POS environments. Services include hosted systems to help you manage electronic payments, as well as professional services to help design, integrate and fully manage parts or all of your payment operations. Over 200,000 businesses worldwide use CyberSource solutions, including half the companies comprising the Dow Jones Industrial Average and leading Internet brands. The company is headquartered in Mountain View, California, and has sales and service offices in Japan, the United Kingdom, and other locations in the United States.

Get Tailored Views of Risk Management Pipeline™ Metrics

A summary of CyberSource's full pipeline process analysis is provided in the Appendix. 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/**

For More Information

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

North America
CyberSource Corporation
1295 Charleston Road
Mountain View, CA 94043
T: 888.330.2300
T: 650.965.6000
F: 650.625.9145
Email: info@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) 118.929.4841
Email: uk@cybersource.com
UK Fraud Report: www.cybersource.co.uk/ukfraudreport

Japan
CyberSource KK
3-25-18 Shibuya, Shibuya-ku
Tokyo, 150-0002 Japan
T: +81.3.4363.4111
F: +81.3.4363.4118
Email: mail@cybersource.co.jp