



8th Annual ONLINE FRAUD REPORT

**Online Payment Fraud Trends,
Merchant Practices & Benchmarks**

2007 Edition

Report & Survey Methodology

This report is based on a survey of 351 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 2006 survey reported a total estimate of \$53 billion dollars for their 2006 online sales. Survey respondents include both non-CyberSource and CyberSource merchants. The survey was conducted via online questionnaire by Mindwave Research. Three hundred and fifty-one organizations completed the survey between September 14th and October 6th, 2006. All participants were either responsible for or influenced decisions regarding risk management in their companies.

Summary of Participants' Profiles

Online Fraud Survey Wave	2002	2003	2004	2005	2006
Total number of merchants participating	341	333	348	404	351
Annual Online Revenue					
Less than \$500K	28%	29%	34%	50%	37%
\$500K to Less than \$10M	44%	43%	39%	24%	30%
Over \$10M	28%	28%	27%	26%	33%
Duration of Online Selling					
Less than One Year	12%	10%	12%	14%	11%
1-2 Years	28%	19%	14%	19%	11%
3-4 Years	45%	44%	30%	23%	18%
5 or More Years	15%	27%	44%	45%	61%
Risk Management Responsibility					
Ultimately Responsible	32%	49%	50%	60%	54%
Influence Decision	68%	51%	50%	40%	46%

Table of Contents

EXECUTIVE SUMMARY	3
STAGE 1: AUTOMATED SCREENING	5
Fraud Detection Tools	5
Planned 2006 Fraud Tool Use	7
Automated Decision/Rules Systems	7
STAGE 2: MANUAL REVIEW	8
Manual Order Review Rates	8
Manual Order Review Efficiency	9
Actions Taken During Review	9
Final Order Disposition	9
STAGE 3: ORDER DISPOSITIONING (ACCEPT/REJECT)	10
Post-Review Order Acceptance Rates	10
Overall Order Rejection Rates	11
STAGE 4: FRAUD CLAIM MANAGEMENT	12
Fighting Chargebacks	12
Chargeback Management Tools	13
Chargebacks—Only Half the Problem	13
Fraud Rate Metrics	14
TUNING & MANAGEMENT	16
Maintaining and Tuning Screening Rules	16
Merchant Budgets for Fraud Management	17
Budget Allocation	17
APPENDIX	18
Sample Risk Management Pipeline Metrics	18
RESOURCES & SOLUTIONS	19
CyberSource Payment Management Solutions	19
ABOUT CYBERSOURCE	20
For More Information	20

Get Tailored Views of Risk Management Pipeline™ Metrics

A summary of CyberSource's full pipeline process analysis is provided in the Appendix of this report. 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/risksolutions**
- **Global Payment & Security Solutions: visit www.cybersource.com/products_and_services/global_payments**

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 eighth 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% measured 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 2006, we estimate that \$3.0 billion in online revenues was lost to online fraud — up from \$2.8 billion in 2005.

Key Fraud Metrics

The percent of accepted orders which are later determined to be fraudulent remained relatively stable. In 2006 the survey shows the overall fraudulent order rate was 1.1% vs

¹ U.S. Census Bureau Retail E-Commerce Sales reports, Forrester Research.

1.0% in 2005. The share of incoming orders merchants declined to accept due to suspicion of payment fraud was up slightly. In 2006 the overall order rejection rate was 4.1% compared to 3.9% in 2005. If only 20% of these turned out to be valid, then as much as another \$1.6 billion may have been lost—most likely to competitors.

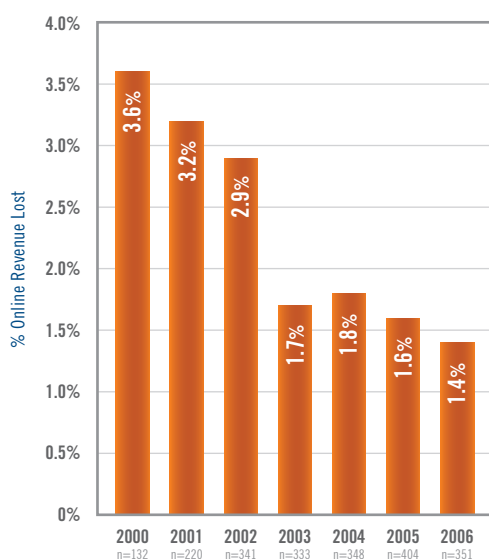
Chargebacks Understate Fraud Loss by as Much as 50%

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 in response to a consumer's claim of fraudulent account use. Overall, merchants continued to report that chargebacks accounted for less than half of fraud losses.

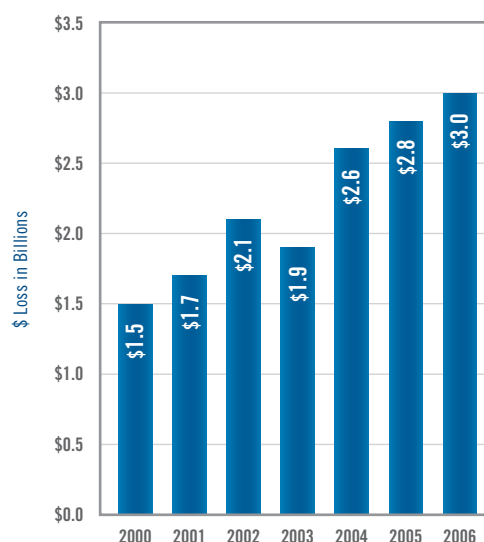
International Order Risk 2 ½ Times Higher Than Domestic Orders

On average, merchants say the rate of fraud associated with international orders is two-and-one-half times as high as domestic orders. Merchants also reject international orders at a rate three times higher than domestic orders. These are the same ratios we found in last year's survey.

% Revenue Lost to Online Fraud



Online Revenue Loss Due to Fraud
\$3.0B in 2006



Although the rate of revenue loss due to online payment fraud has declined in 2006, total dollars lost to fraud have increased due to increased online sales growth.

Manual Review Rates Fall

After reaching a plateau in 2005, manual review rates experienced their first significant decline in 2006. After steadily increasing from 2000 to 2004, manual review rates declined from 26% of orders in 2005 to 23% of total orders in 2006. Overall, 81% of merchants are engaging in manual order review. Merchants who see less than \$5 million in annual online orders have the highest review rate (average 36% of orders). On average, medium and large merchants (merchants selling more than \$5 million online) review 15-25% of orders and seek productivity gains through automation. Medium and large merchants tend to employ two times the number of screening tools as compared to smaller merchants and are two times as likely to utilize automated decision systems.

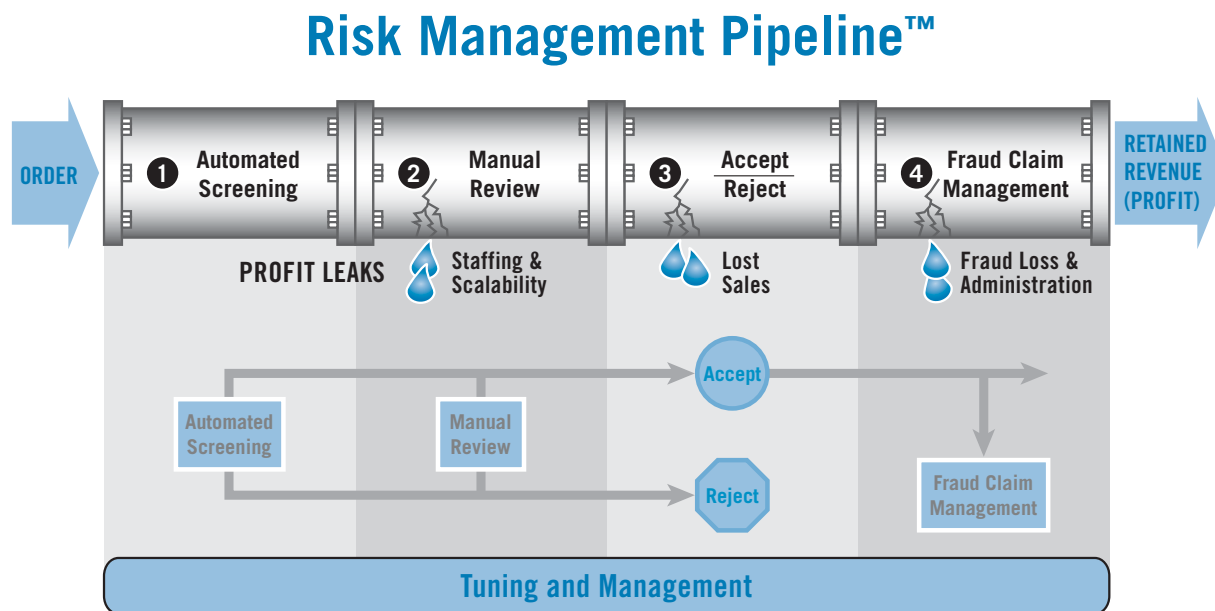
Efficiency Gains of As Much As 20% May Be Required

As online eCommerce sales continue to grow 20% or more per year, larger merchants face the growing problem of screening more online orders. Continued reliance on manual review presents a serious challenge to scalability. Only 24% of larger online merchants report having budget to increase manual review staff in 2007 to cope with higher order volumes. Therefore, each year, larger merchants must increase fraud management efficiency approximately 20% just to keep pace.

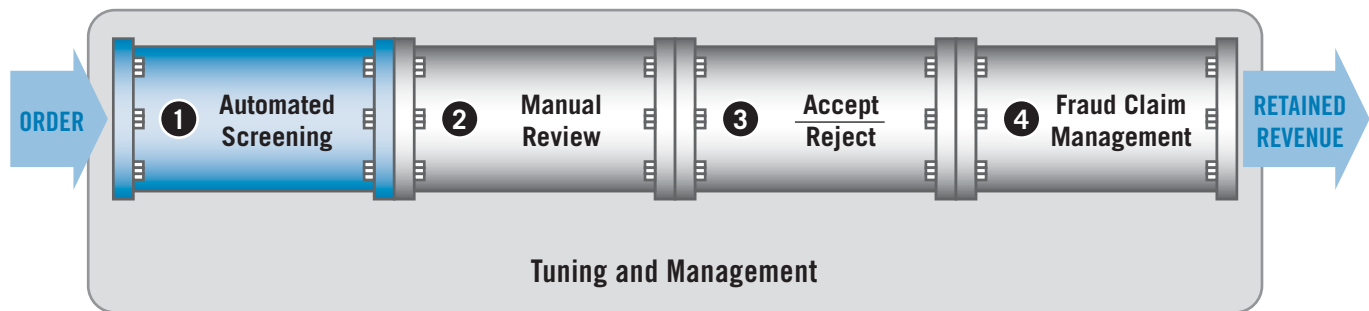
Total Pipeline View

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 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 association limits), an end-to-end view is required to arrive at the best possible financial outcome.

In 2006, these “profit leaks” in the Risk Management Pipeline™ impacted as much as 30+% of orders for medium merchants and as much as 20+% 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.



Stage 1: Automated Screening



Fraud Detection Tools

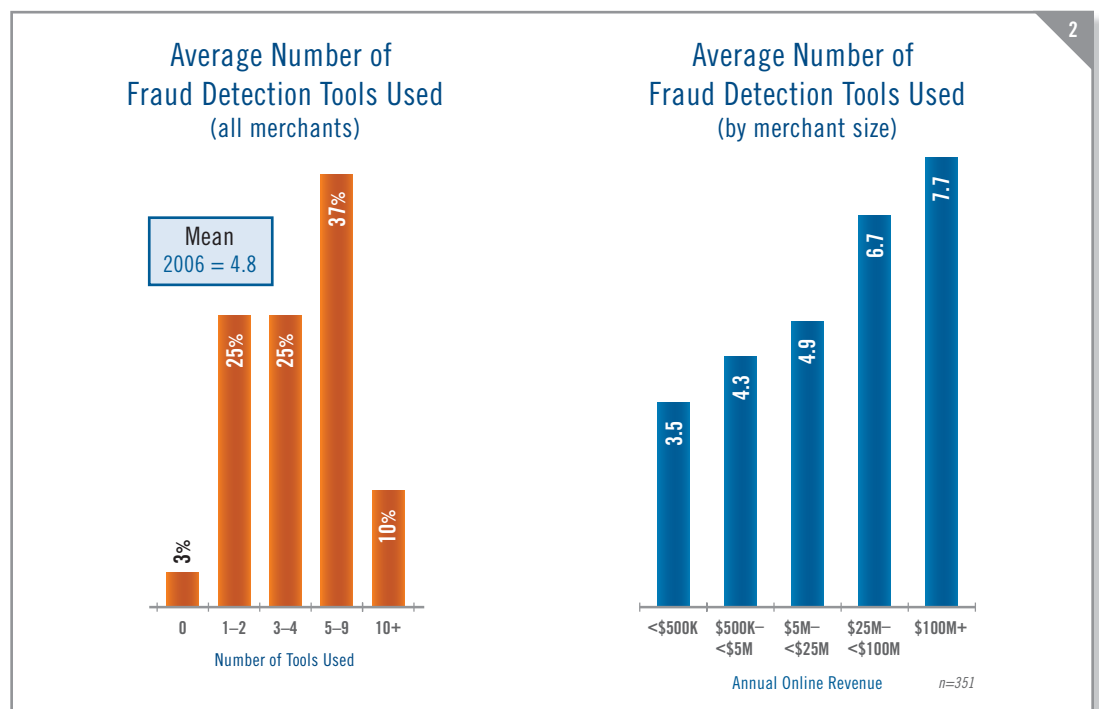
We define detection tools as those used to identify the probability of risk associated with a transaction or to validate the identity of the purchaser. Results of tests carried out by detection tools are then interpreted by humans or rules systems to determine if a transaction should be accepted, rejected or reviewed. A wide variety of tools are available to help merchants evaluate incoming orders for potential fraud. In 2006, over two-thirds of merchants reported using three or more fraud detection tools, with 4.8 tools being the average. 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 (see page 6) 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.

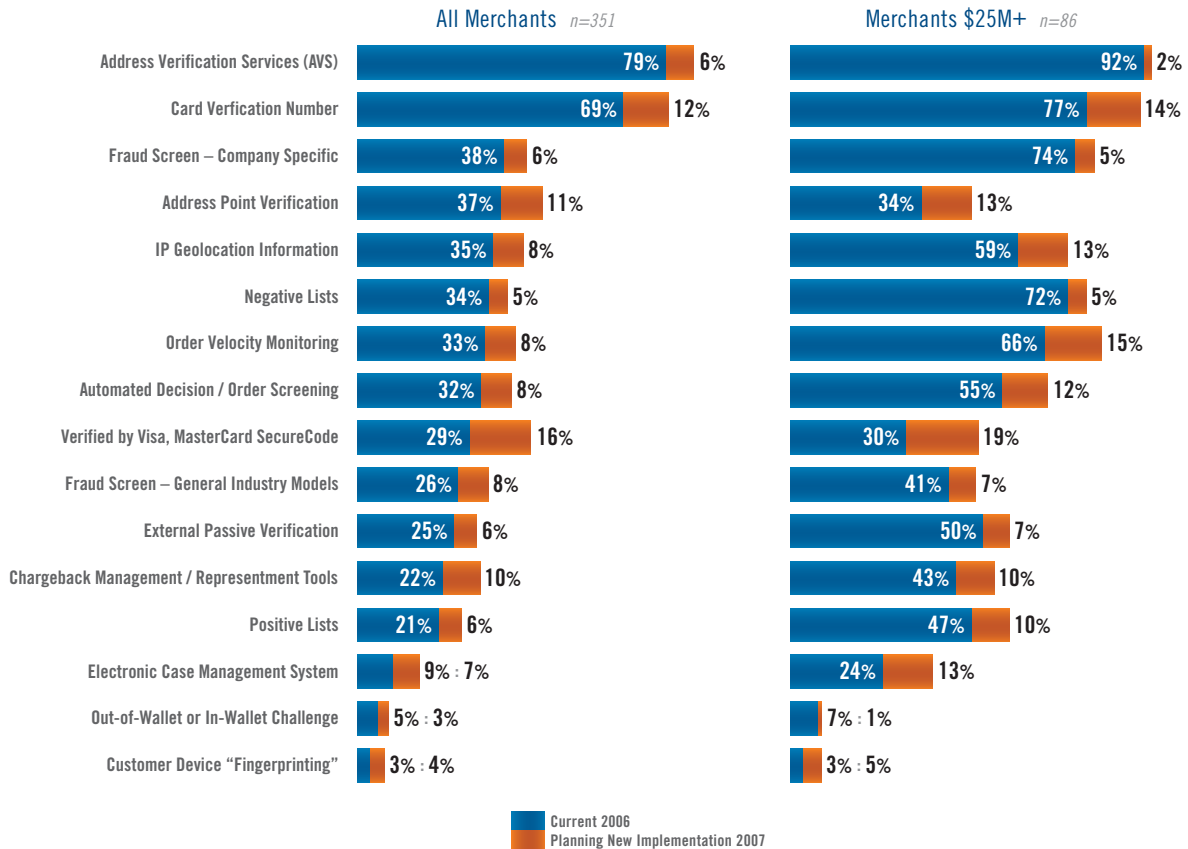
The use of basic fraud detection tools has continued to increase in 2006. The tool most often mentioned by merchants is the Address Verification

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. 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 the AVS result to accept or reject an order.



Current & Planned Fraud Detection Tool Usage



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 69% today.

Most fraud management tools experienced an increase in adoption in 2006 with IP geolocation, company specific fraud screens and order velocity monitoring showing the highest increases in adoption (all up by 10 pts). Interesting and emerging fraud tools this year include in/out of wallet challenges (where online buyers are asked specific background questions during the online order process) and device fingerprinting (which examines and records details about the configuration of the internet device the order is being placed from). Both of these are in their infancy with adoption rates of less than 10% of merchants surveyed.

Planned 2007 Fraud Tool Use

Payer Authentication Services Cited As Tool Most Often Planned For Implementation in 2007

Card association payer authentication services (e.g. Verified by Visa, MasterCard SecureCode) figure prominently in many merchants' future plans. Over the last few years, survey data indicates a steady increase in the adoption of payer authentication systems, rising from 19% in 2003 to 29% in 2006. 16% of respondents say they are interested in deploying these systems in 2007 as a new tool to detect and manage fraud. 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). 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

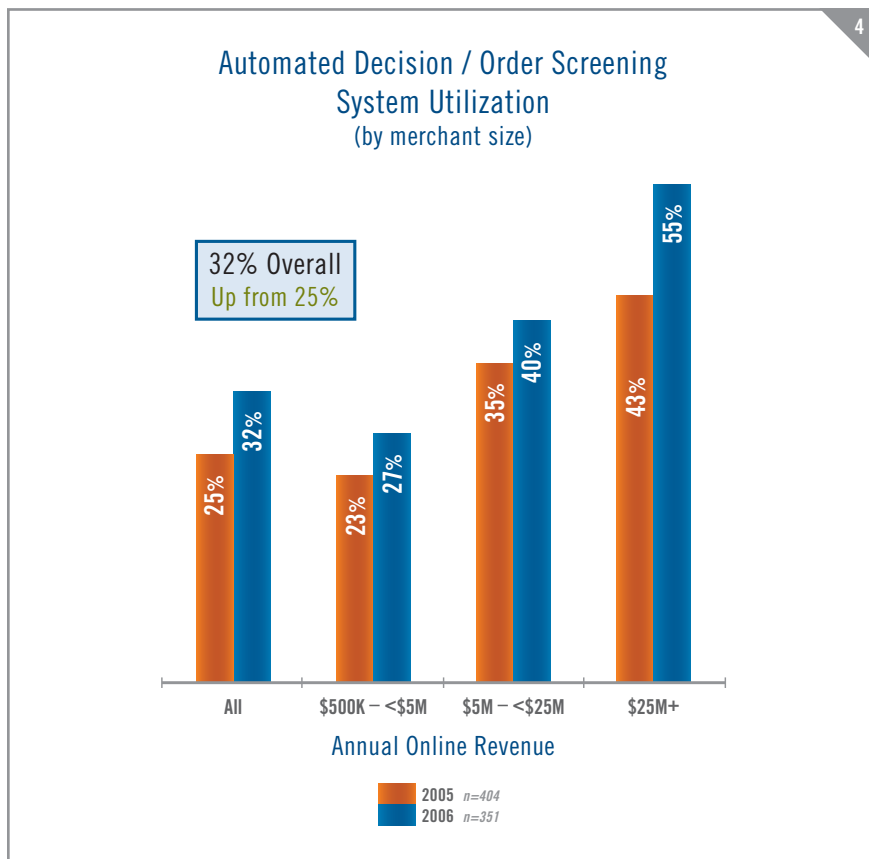
procedures in place to handle customers who have not adopted the new systems or who use cards which are not yet supported. The growing popularity of online payment types such as electronic checks, PayPal, Bill Me Later, etc. will also require different fraud management techniques.

Automated Decision/Rules Systems

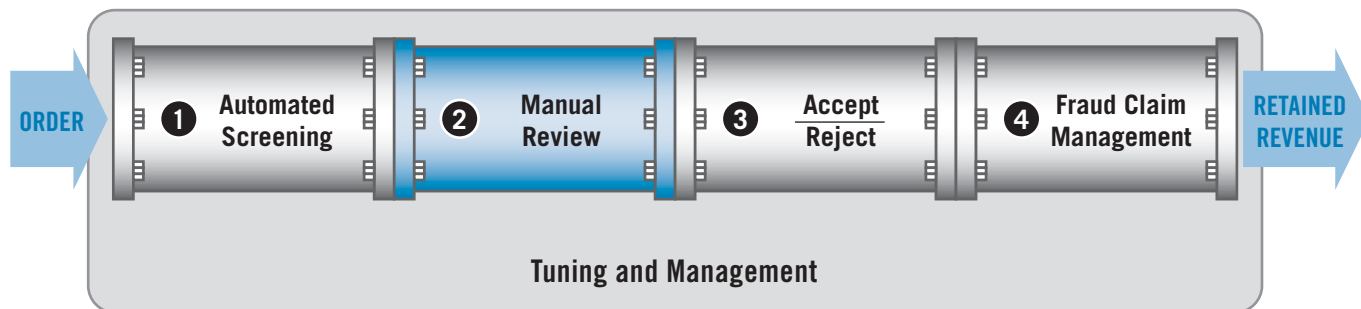
Automated Order Screening

Automated order decisioning / screening is now used by 32% of merchants (up from 25% in 2005). Over 50% 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, 8% of merchants say they plan to add this capability in 2007. 12% 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.



Stage 2: Manual Review



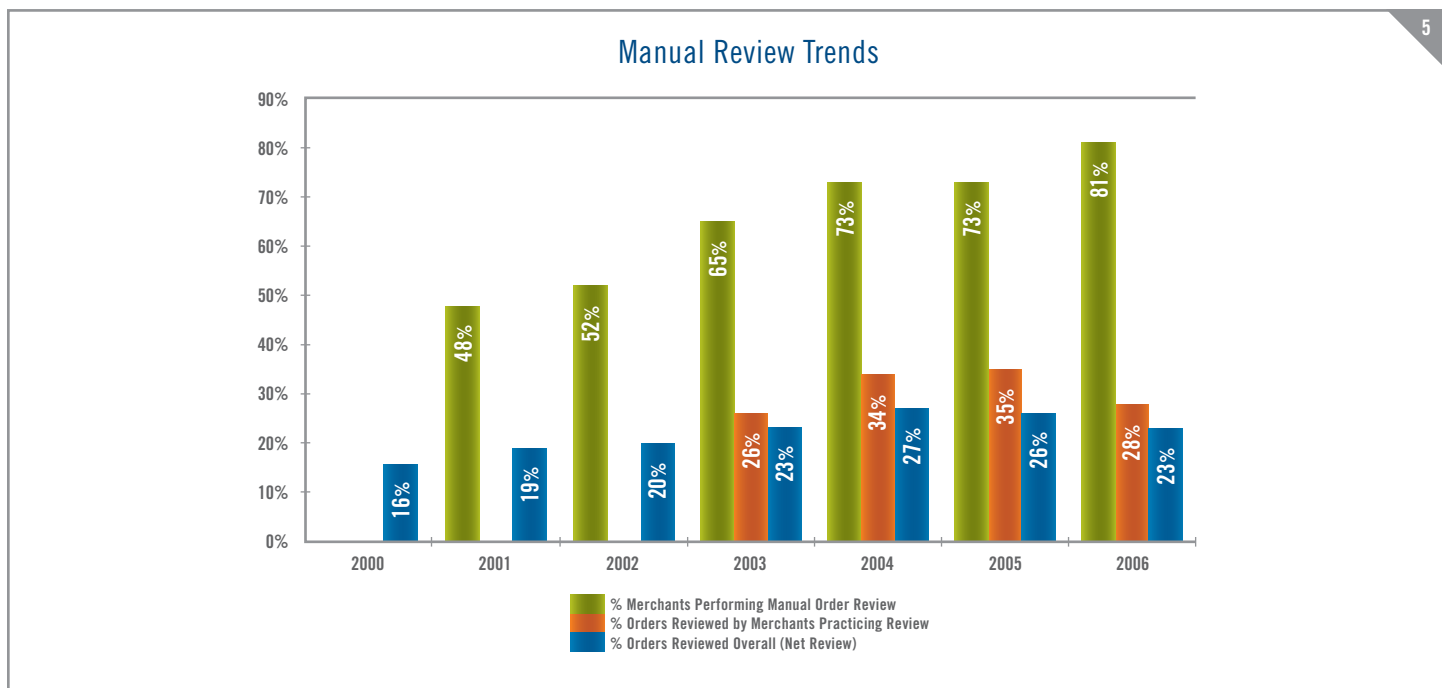
Orders which do not pass the automated order screening stage typically enter a manual review queue. During this stage, additional information is collected about the order to determine if it should be accepted or rejected due to excessive fraud risk.

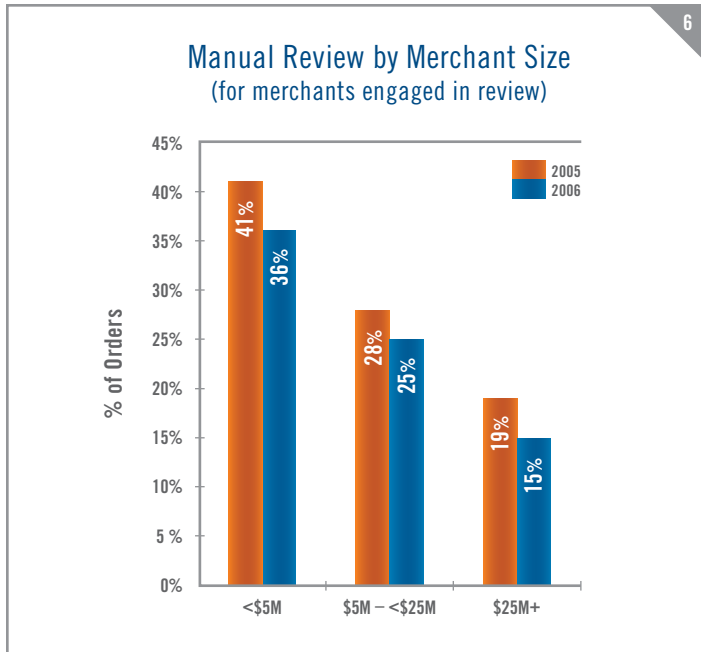
Manual review represents a critical area of profit leakage. It is expensive, limits scalability and impacts customer satisfaction. Few merchants say they have budget available to increase review staff now or in the next twelve months. Even at a stable percent of orders sent to review, the total number of orders that must be reviewed increases in step with total online sales increases.

Manual Order Review Rates

In what should be a highly automated sales environment, 81% of merchants are manually checking orders today. Their average rate of manual review exceeds 1 out of 4 orders. Projecting this rate across all merchants and orders, approximately 23% of all online orders (about one in four) were reviewed in 2006, as compared to 16% in 2000 (approximately one in six orders).

Merchants of all sizes use manual review to manage payment fraud. Chart #6 (see page 9) shows smaller merchants review a higher percentage of orders (perhaps because lower order volumes permit such practice) but



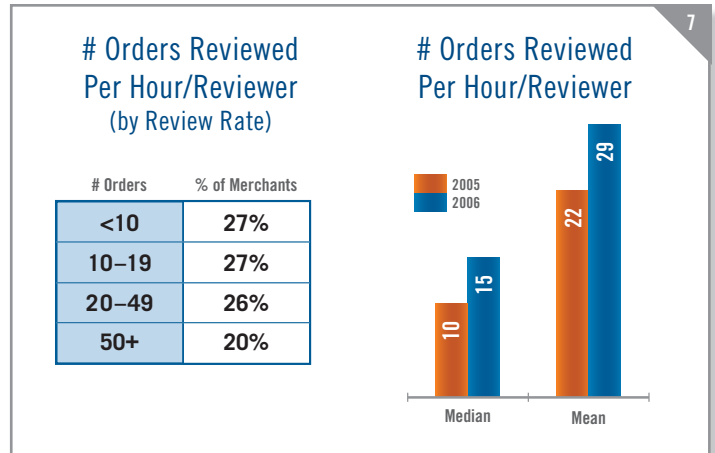


even larger merchants review a significant percentage of online orders—and likely devote more resources to this task than is operationally scalable.

While the percentage of online orders being manually reviewed was down in 2006 for those merchants doing manual review, the volume of online sales is up (according to most sources) by 20% or more. Virtually all online sales forecasts continue to project high growth rates over the next few years. As a result, 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

In 2006, survey data shows that 54% of companies review less than 20 orders per hour, per reviewer. On average, larger merchants say they review more orders per hour than smaller merchants. This difference may be attributed to a higher utilization of case management systems among larger merchants. 24% of merchants over \$25 million in annual online sales report use of case management systems, nearly three times the overall rate of 9%.



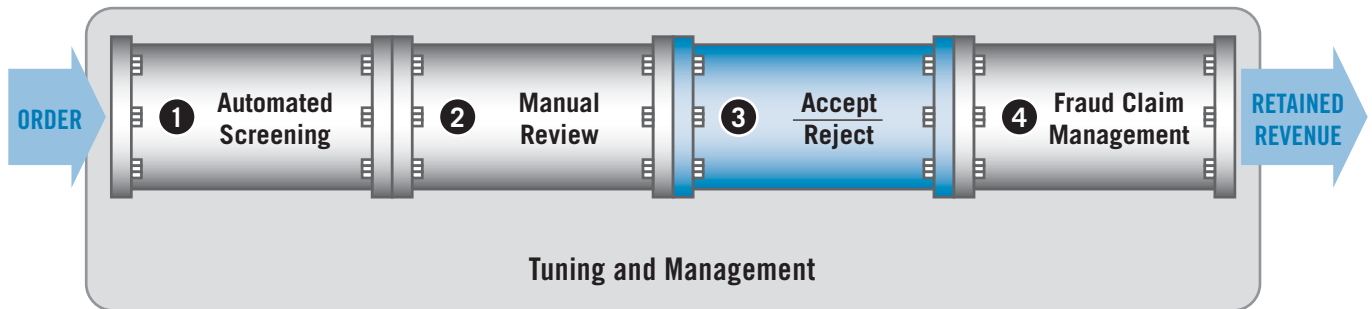
Actions Taken During Review

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 the customer. In last year’s 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

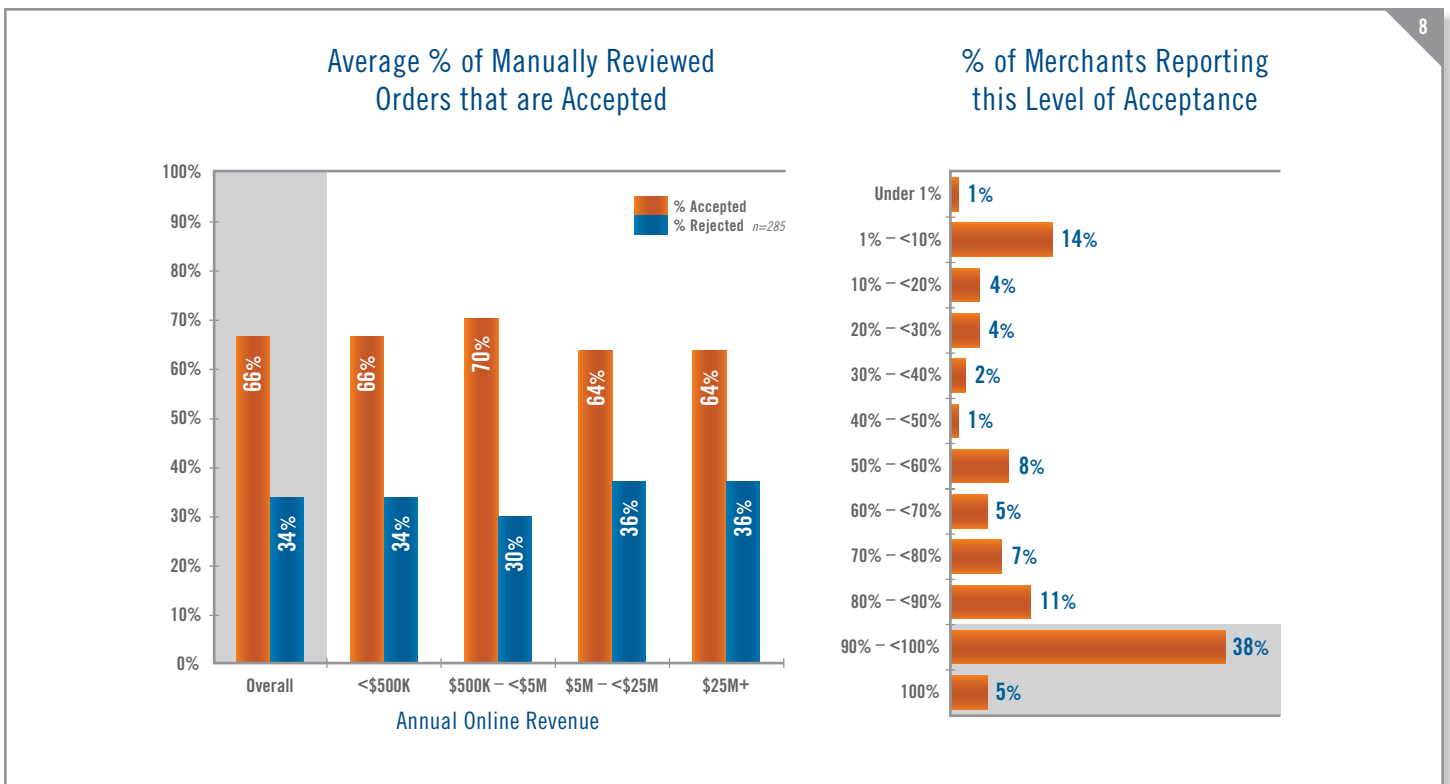
Automated screening and manual order review ultimately result in order acceptance or rejection. A relatively high percentage of orders reviewed are ultimately accepted (see next section)—highlighting the need for merchants to improve automated screening and reduce the need for review. A look at order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

Stage 3: Order Dispositioning (Accept/Reject)



Post-Review Order Acceptance Rates

In 2006, merchants surveyed indicated that they ultimately accepted over two-thirds of the orders they manually reviewed (see chart #8). Over 40% of merchants report they accept 90% or more of orders they manually review.



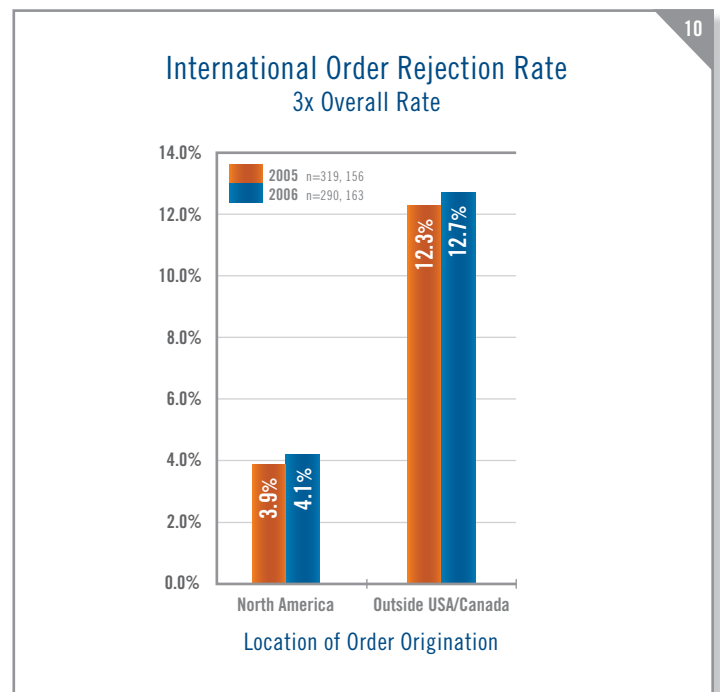
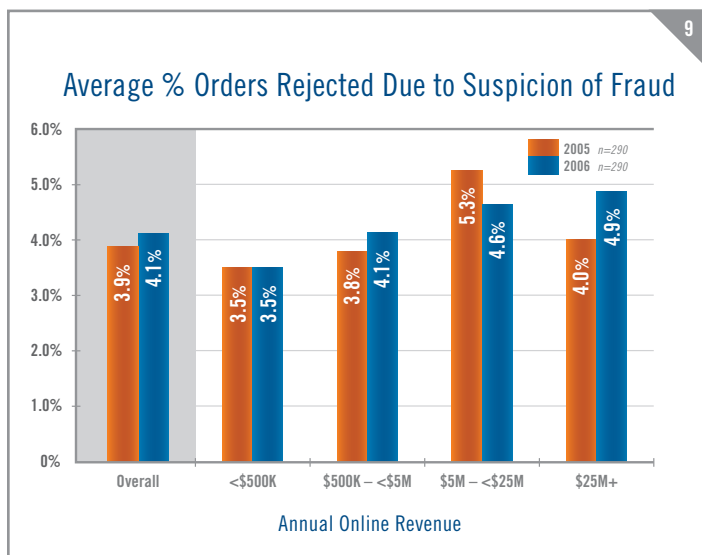
Overall Order Rejection Rates

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 2006, merchants participating in the survey reported a slight increase in their order rejection rates from 3.9% in 2005 to 4.1%. For every fraudulent order they received they rejected almost 4 orders due to suspicion of fraud.

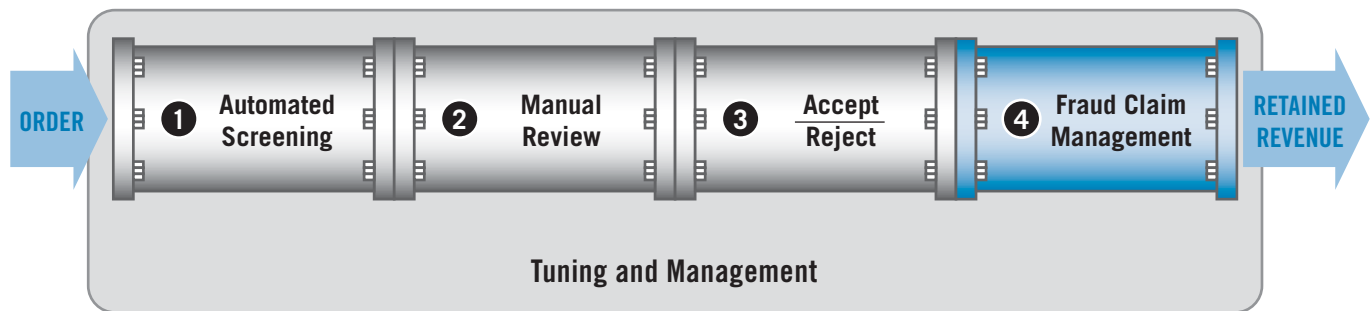
Large online merchants, who saw a 0.3% point drop in their accepted fraud rate, saw a significant increase in their order rejection rate, which rose from 4.0% in 2005 to nearly 4.9% in the 2006 survey. From 2005 to 2006, the largest merchants appear to have avoided one incremental fraudulent order by rejecting an additional 3 orders. If the combined total gross margin on the 3 rejected orders was less than the cost of one fraudulent order (eg. cost of goods sold + shipping and handling costs) then these merchants have set their order acceptance criteria and risk thresholds at an appropriate level. However, to the extent the lost gross margin on the 3 rejected orders is larger than a single fraudulent order there may be room for increasing bottom line profit by further tuning acceptance and risk thresholds (see our whitepaper “Managing eCommerce Payment Fraud”). Sophisticated merchants realize it is possible to “over control” fraud losses at the expense of net gains in

revenues and profits. Effective fraud management involves careful optimization of all the fraud metrics.

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. Again in 2006 merchants report their rejection rate on these orders is three times higher than for domestic orders as shown in chart #10 below. The actual fraud rate experienced on international orders seems to support this cautious approach; merchants report the fraud rate on international orders is over twice that of domestic orders (see chart #18).



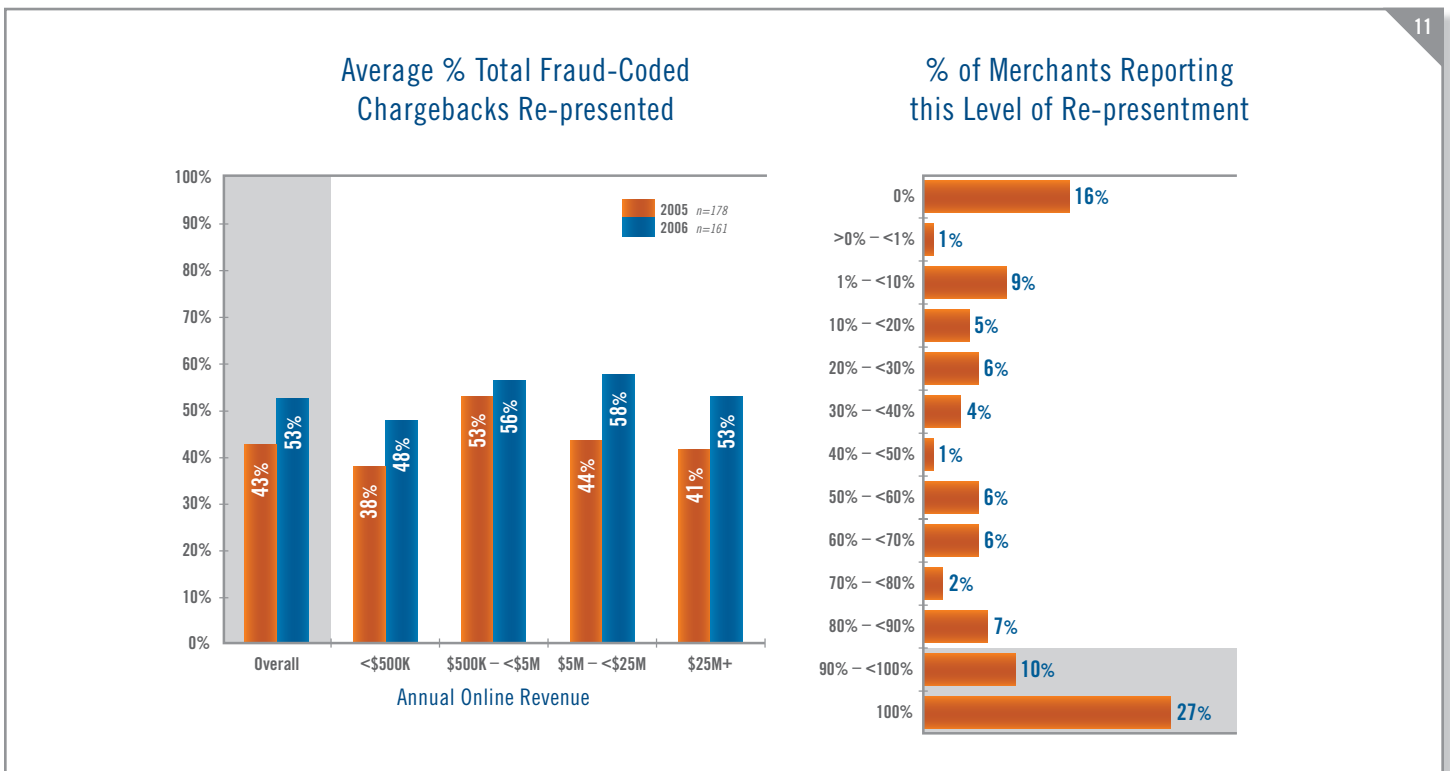
Stage 4: Fraud Claim Management

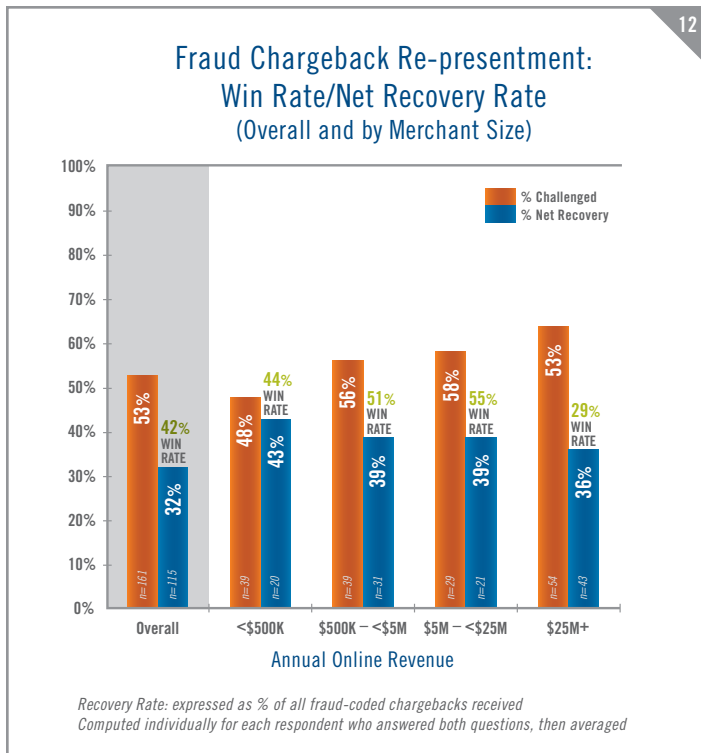


Fighting Chargebacks

This year's survey also examined practices associated with reviewing and contesting chargebacks ("re-presentation"). Overall, an average of 53% of fraud-coded chargebacks are re-presented (up from 43% in 2005), with over one-in-three merchants contesting 90-100% of chargebacks and one-in-four contesting fewer than 10% (see chart below).

Merchants report that they win, on average, 42% of the chargebacks they dispute. These averages translate to an overall net recovery rate of 22% (meaning 22% of all fraud-coded chargebacks are recovered). However, given the wide disparity in the chargeback re-presentation rate, when these are calculated on a merchant-by-merchant basis and then averaged, the re-presentation win rate rises to 32%. So, nearly one out of three fraud chargebacks are recovered upon re-presentation (see chart #12 on next page). Clearly, having an efficient re-presentation process can help enhance profitability and reduce fraud loss.





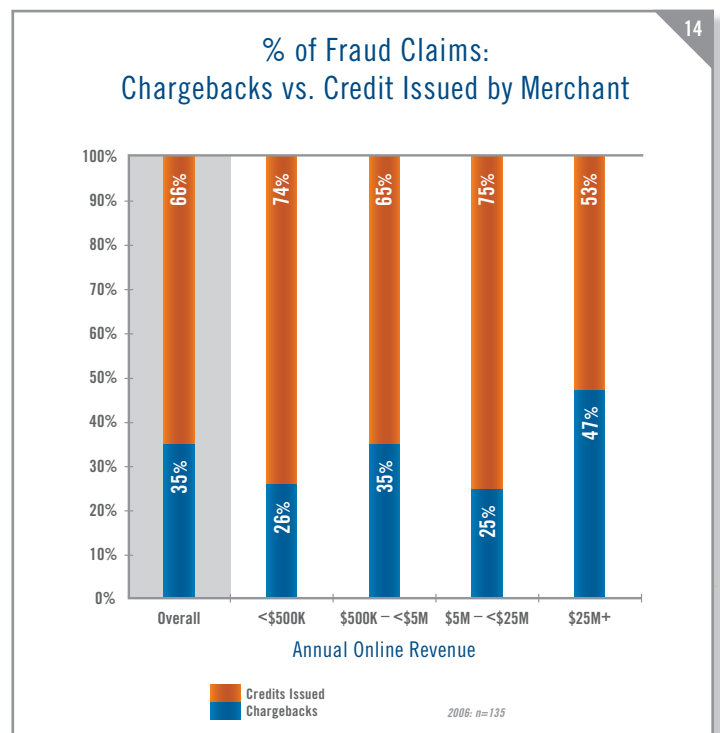
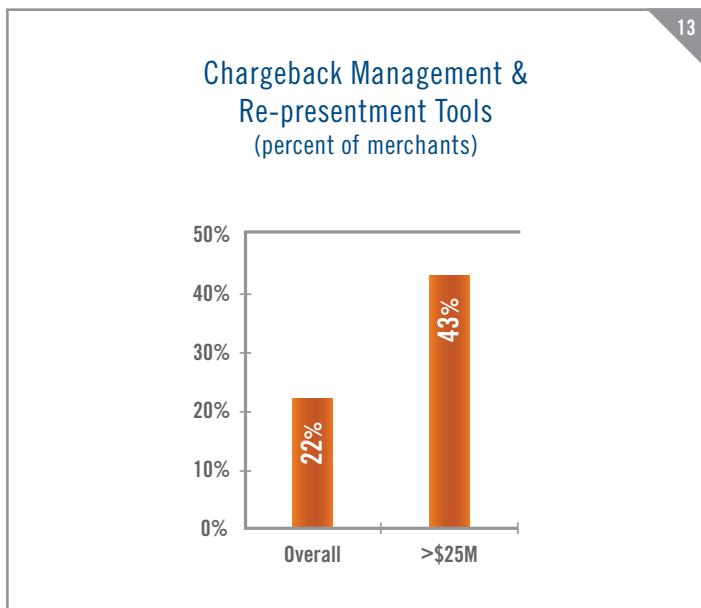
this aspect of the pipeline. As chart #13 shows, larger merchants, managing higher volumes of fraudulent orders, tend to invest in automated re-representation tools more than the average online merchant. In 2006, merchants provided estimates of how many hours it takes, on average, to handle a fraud chargeback. 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 talked about metric, merchants report that chargebacks actually account for less than half of all fraud claims. This is true for all sizes of merchants (see chart below).

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



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. Further, 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 the phenomenon of 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. The survey data supports that

risk practices vary widely by type of online merchant. 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 #15). 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).

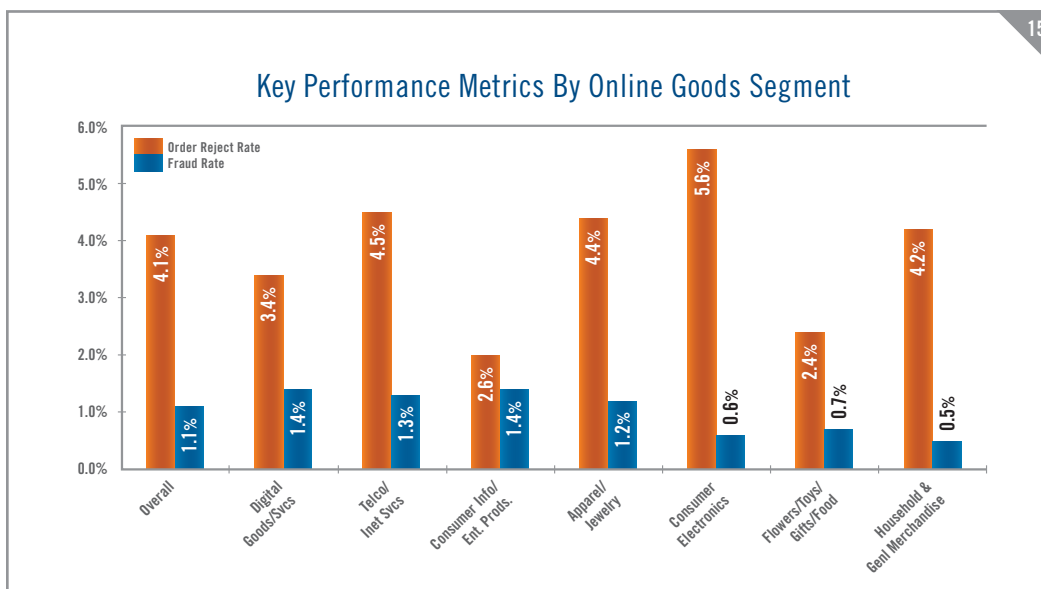
Direct Revenue Loss Rates

Revenue loss rates vary by a merchant's online revenue size. 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.

Fraudulent Order Rate for Accepted Orders

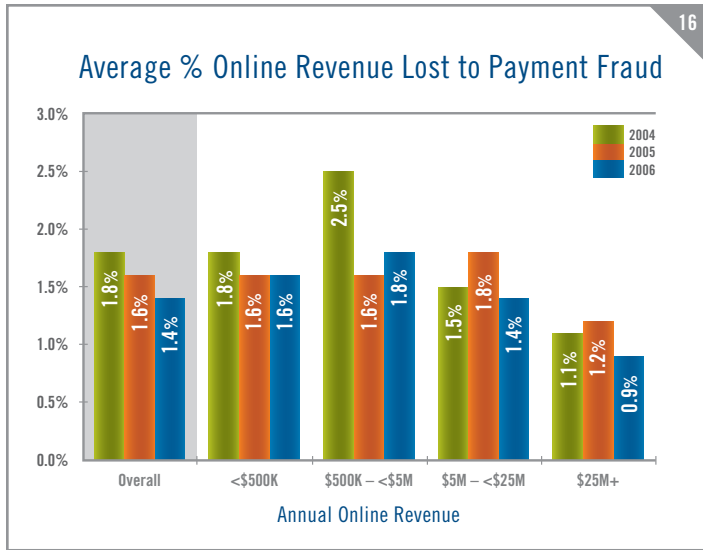
Another key metric is the number of accepted orders that later turn out to be fraudulent. Expressed as a percent of total orders, this metric is typically lower than the revenue loss percent since the average value of fraudulent orders tends to be greater than the average value of valid orders, which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

to be higher. Overall, 39% of merchants report experiencing a fraudulent order rate of 1% or more in both 2005 and 2006 survey data.

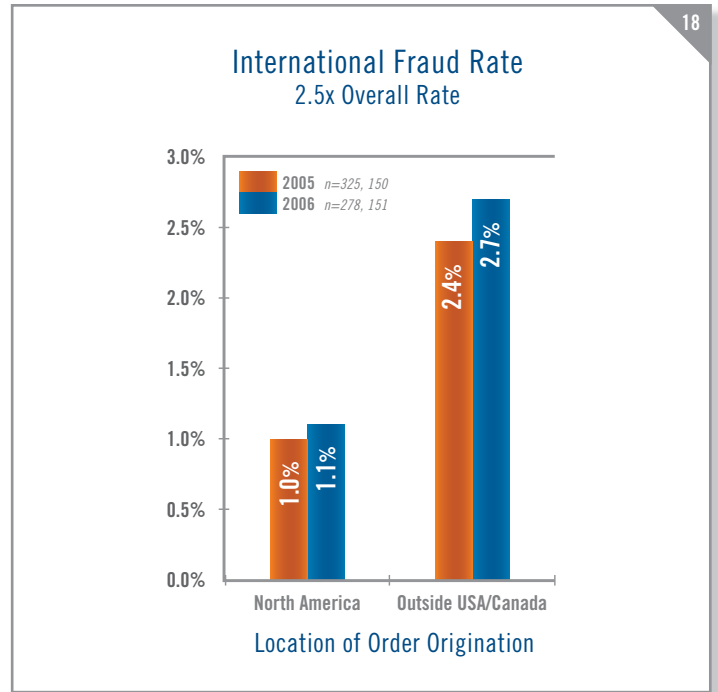


International Orders Carry Higher Risk

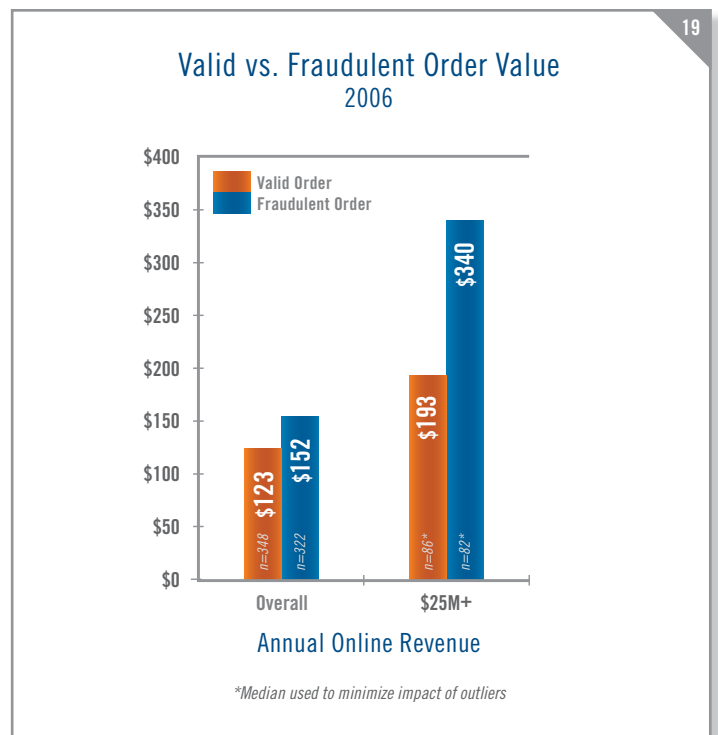
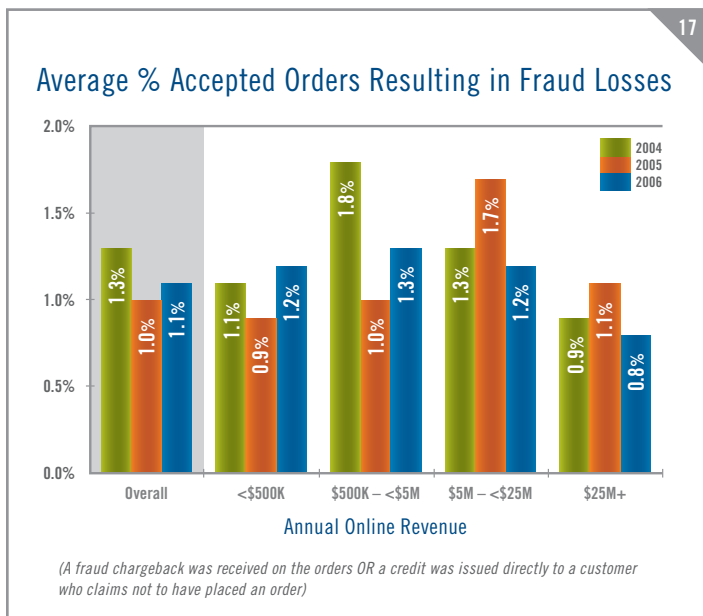
Sixty-one percent of merchants surveyed accepted orders from outside the U.S. & Canada in 2006. International sales accounted for an average of 17% of total orders for these merchants. That same group reported that the actual direct fraud rate on



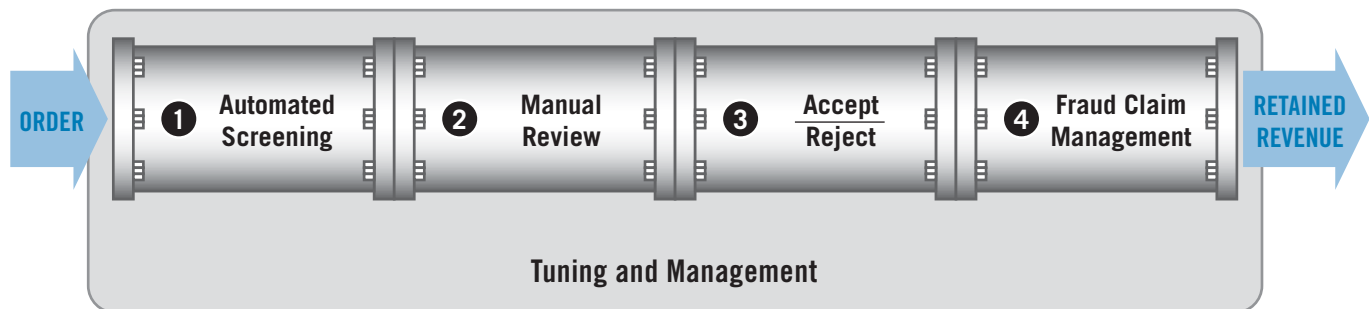
international orders averaged 2.7%, or more than twice the overall fraud rate for domestic online orders. While online sales in the U.S. are still growing by 20% or more each year, sales in Europe and many other markets are showing even higher growth. Though international markets represent an attractive 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 three times the domestic rate of 4.1% — rejecting approximately 1 out of every 8 international orders received.



Average Value of Fraudulent Order Higher than a Valid Order
The median value of a fraudulent order in the survey was \$152 or 24% higher than the \$123 median value of a valid order.

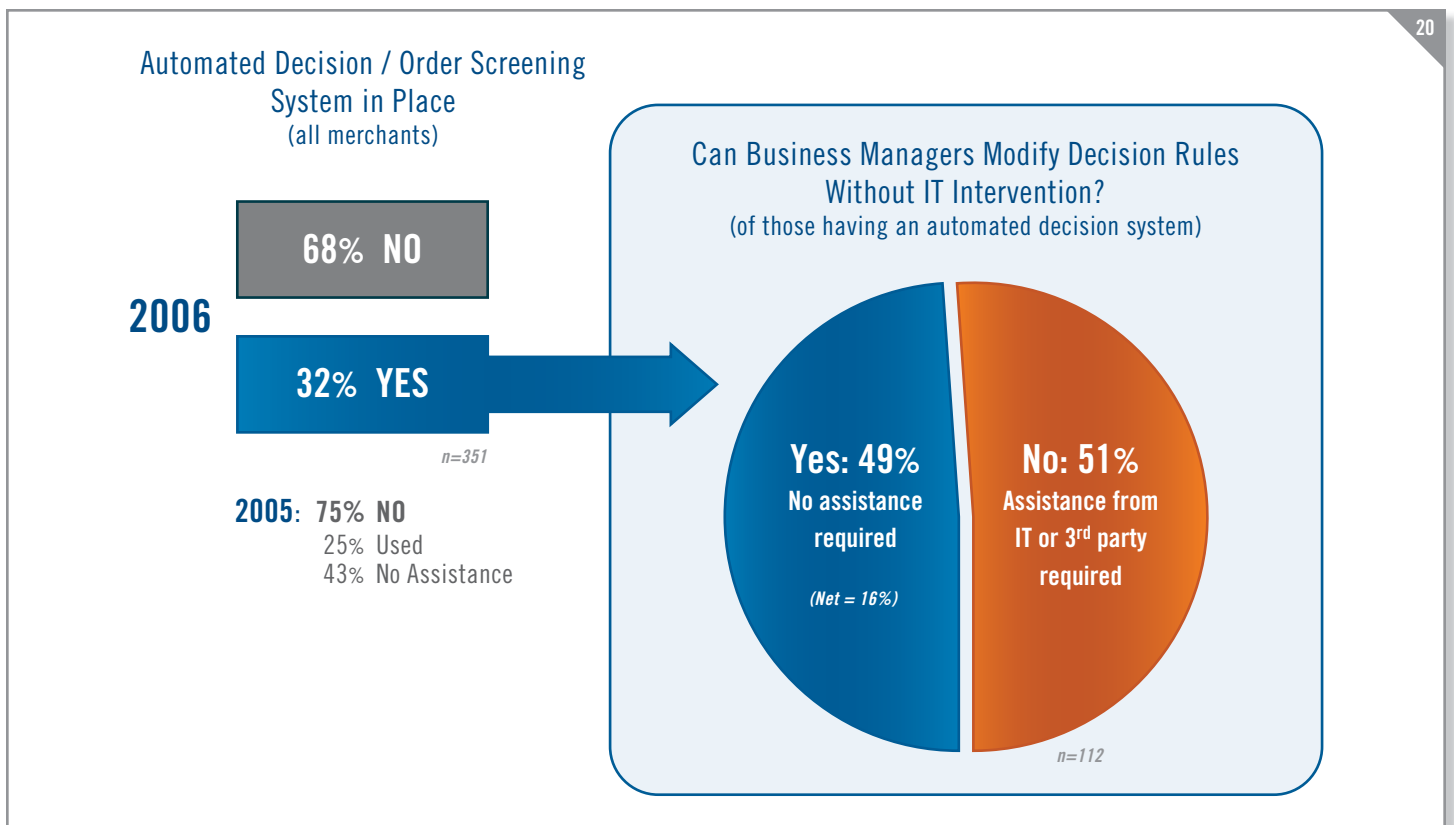


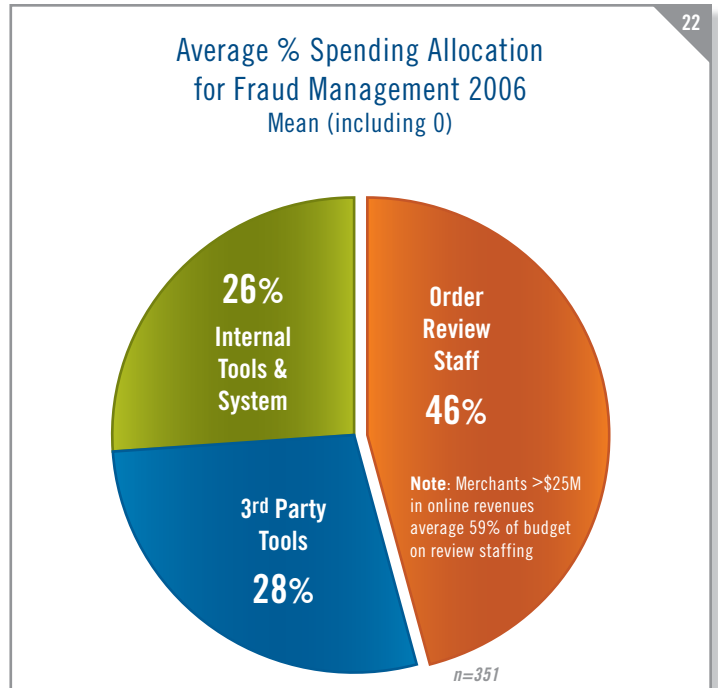
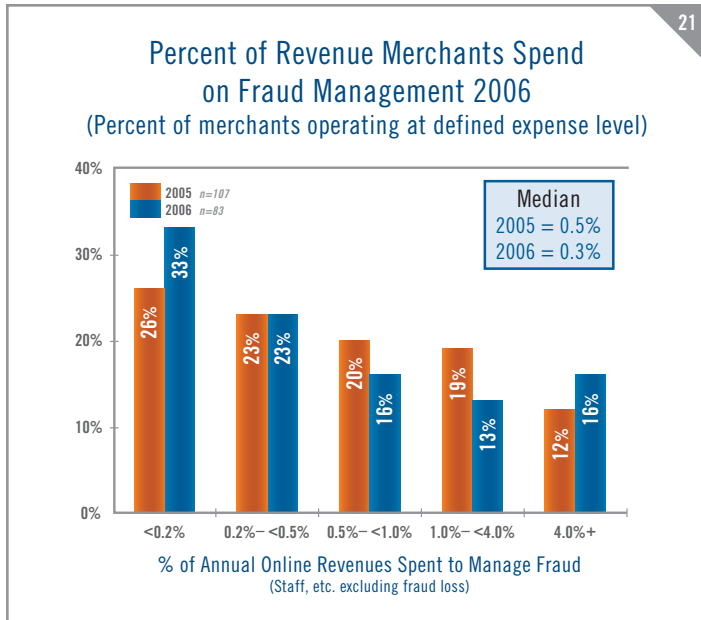
Tuning & Management



Maintaining and Tuning Screening Rules

Among merchants having an automated order screening system in place, 49% have systems that allow business managers to modify decision rules without assistance from internal IT staff or external third parties (meaning overall, only 16% of all merchants have systems in place allowing 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 to adjust business rules on the fly reduces the costs and burden of IT support.



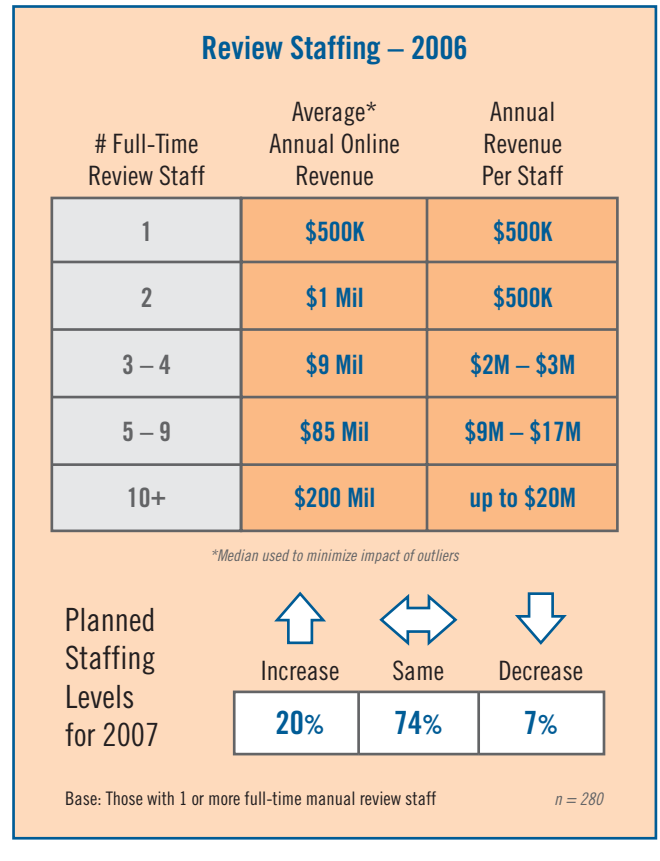


Merchant Budgets for Fraud Management

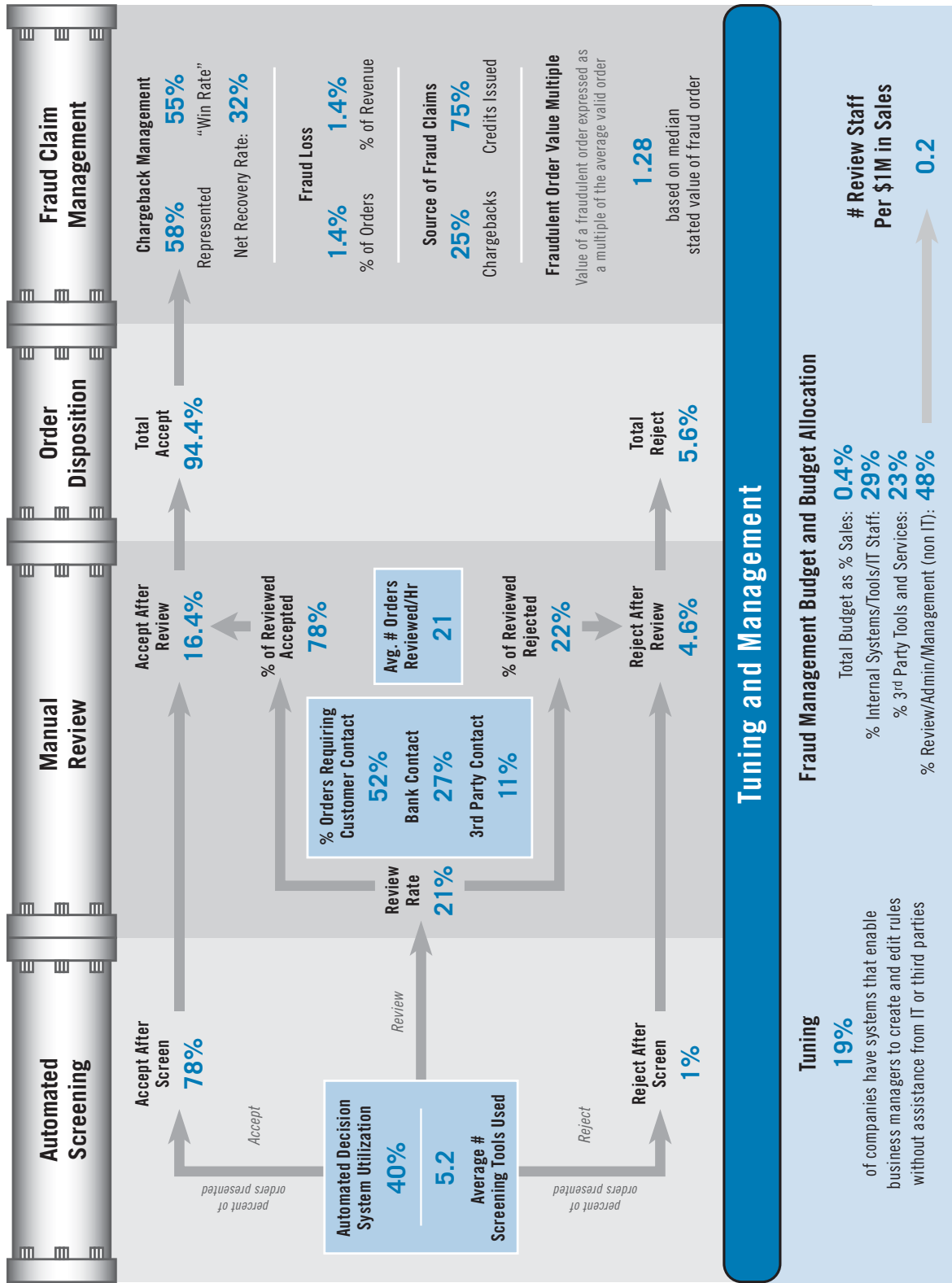
How much are online merchants spending to mitigate fraud risk? Forty-four percent of merchants spend 0.5% or more of their online revenues to manage online payment fraud while 56% spend less than 0.5%. Across all merchants, the median ratio of fraud management expense to sales ranges from 0.3% in this year's survey to 0.5% reported in 2005, 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 and development staff, and review staffs). Direct fraud loss (chargebacks/credits, lost goods and associated shipping costs), as well as the opportunity cost associated with valid order rejection are not included here. (See chart #21)

Budget Allocation

On average, order review staff costs consume 46% of the fraud mitigation budget (see chart #22). The remainder is allocated as follows: 28% for third party tools or services and 26% 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.



APPENDIX: Sample Risk Management Pipeline Metrics \$5M – \$25M



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

© 2007 CyberSource Corporation. All rights reserved. The Risk Management Pipeline is a trademark of CyberSource Corporation.

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 sales results.

Payment Acceptance

Merchant accounts for domestic and global payment acceptance, including: 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

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. Optionally, you can use our decision and case management systems, and robust array of fraud detection and verification tools (risk scoring, Verified by Visa/MasterCard SecureCode, IP Geolocation, Address Validation, identity morphing detection, device mapping, and more) to streamline fraud management using your own internal resources.

Processing Management

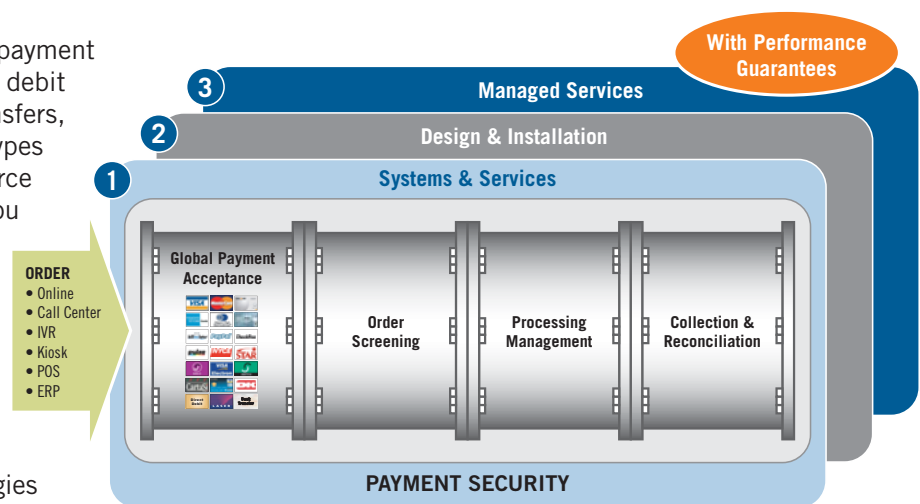
CyberSource provides on-demand access to over 45 processors (over 120 countries) around the globe. CyberSource's highly reliable, triple-redundant datacenters are PCI-compliant worldwide and include sophisticated processing management capability to prevent subscription payment failures and rate downgrades.

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-presentation.

Payment Security

CyberSource provides secure storage and hosted payment acceptance services to help you bolster payment security and streamline PCI compliance. We also provide 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 management and payment security solutions. CyberSource solutions enable electronic payment processing for Web, call center, and POS environments. CyberSource also offers industry leading risk management solutions for merchants accepting card-not-present transactions. CyberSource Professional Services designs, integrates, and optimizes commerce transaction processing systems. Thousands of businesses use CyberSource solutions, including half the companies comprising the Dow Jones Industrial Average. The company is headquartered in Mountain View, California, and has sales and service offices in Japan, the United Kingdom, and other locations in the United States.

Get Tailored Views of Risk Management Pipeline™ Metrics

A summary of CyberSource's full pipeline process analysis is provided in the Appendix of this report. 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/risksolutions
- **Global Payment & Security Solutions:** visit www.cybersource.com/products_and_services/global_payments

For More Information

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

Thank you for reading CyberSource's 8th Annual Fraud Report. This is your chance to let us know whether this annual fraud report is of use to you and the industry. By participating in this brief survey, you have the opportunity to share your opinion. Your input is appreciated. Please take our survey at www.cybersource.com/fraudreportsurvey

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) 870.460.1931
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