

# 7<sup>th</sup> Annual ONLINE FRAUD REPORT

Online Payment Fraud Trends  
Merchant Practices & Benchmarks

2006 Edition

Sponsored by CyberSource Corporation



Power of  
Payment  
Series

CyberSource®  
the power of payment

## Report & Survey Methodology

This report is based on a survey of 404 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 in the world with many years of experience. Merchants participating in the 2005 survey reported a total estimate of \$28 billion dollars for their 2005 online sales. Survey respondents include both non-CyberSource and CyberSource merchants.

The survey was conducted via online questionnaire by Mindwave Research. Four hundred and four organizations completed the survey between September 16th and October 6th, 2005. 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
Total number of merchants participating	341	333	348	404
<b>Annual Online Revenue</b>				
Less than \$500K	28%	29%	34%	50%
\$500K to Less than \$10M	44%	43%	39%	24%
Over \$10M	28%	28%	27%	26%
<b>Duration of Online Selling</b>				
Less than One Year	12%	10%	12%	14%
1-2 Years	28%	19%	14%	19%
3-4 Years	45%	44%	30%	23%
5 or More Years	15%	27%	44%	45%
<b>Risk Management Responsibility</b>				
Ultimately Responsible	32%	49%	50%	60%
Influence Decision	68%	51%	50%	40%

## Table of Contents

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

## Get Tailored Views of Risk Management Pipeline™ Metrics

A summary full pipeline process analysis is provided in the Appendix of this report. 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](http://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](http://www.cybersource.com/contact_us)**
- **Risk Management Solutions: visit [www.cybersource.com/risksolutions](http://www.cybersource.com/risksolutions)**
- **Global Payment Solutions: visit [www.cybersource.com](http://www.cybersource.com)**

# 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 seventh annual survey.

## Overview

Over the past few years the percent of online revenues lost to payment fraud has been relatively stable; ranging from 1.8% in 2004 to 1.6% 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.<sup>1</sup> In 2005, we estimate that \$2.8 billion in online revenues will be lost to online fraud — up from \$2.6 billion in 2004.

## Fraud Experience Different for Medium and Large Merchants vs. Small

Although smaller merchants continue to experience fraud rates that are higher than those for medium and larger merchants, smaller merchants' rate of fraud loss declined during 2005. Conversely, merchants with annual online revenues over \$5 million, on average, experienced a slight increase in revenue loss rates as compared to 2004. In particular, merchants having revenues between \$5-\$25

million experienced the greatest increase in loss rates—possibly because they are most operationally challenged. These companies are most likely to be migrating from a “lower volume, high manual review” environment to a “higher volume, struggling to automate” environment. That said, medium and large online merchants appear to be coming out ahead by accepting slightly more fraudulent orders. Their fraud rate advanced somewhat, but they also accepted more valid orders in total. It is possible that medium and large merchants are more closely examining the trade-off between valid order rejection and fraud acceptance, and making a bottom-line “net profit” decision in the face of operational realities.

## Chargebacks Understate Fraud Loss by as Much as 50%

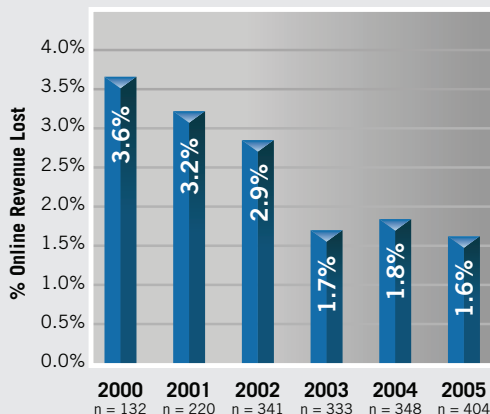
This year's survey probed the percent of fraud losses accounted for by chargebacks versus those incurred as a result of merchants issuing credit in response to a consumer's claim of fraudulent account use. Overall, merchants reported that chargebacks accounted for less than half of fraud losses.

## International Order Risk 2-3 Times Higher

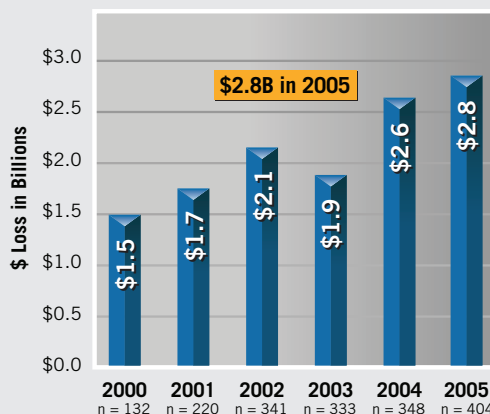
On average, merchants say the rate of fraud associated with international orders is twice as high as the overall average. Further, merchants reject international orders at a rate three times higher than the overall average.

<sup>1</sup> U.S. Census Bureau Retail E-Commerce Sales reports, Forrester Research.

### % Revenue Lost to Online Fraud



### Online Revenue Loss Due to Fraud



Although the rate of revenue loss due to online payment fraud has declined in 2005, total dollars lost to fraud have increased due to increased online sales growth

## Manual Review Rates Stabilize, But Merchants Review More Orders

In 2005, manual review rates stabilized after steadily increasing for the previous four years. Overall, 73% of merchants are engaging in manual order review. Merchants with less than \$5 million in annual online orders have the highest review rate (average 28% 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 2006 to cope with higher order volumes. Therefore, each year, larger merchants must increase fraud management efficiency approximately 20%—just to maintain their current level of business productivity. Arguably, even the current level of operations efficiency is non-optimal. Thus, gains in fraud

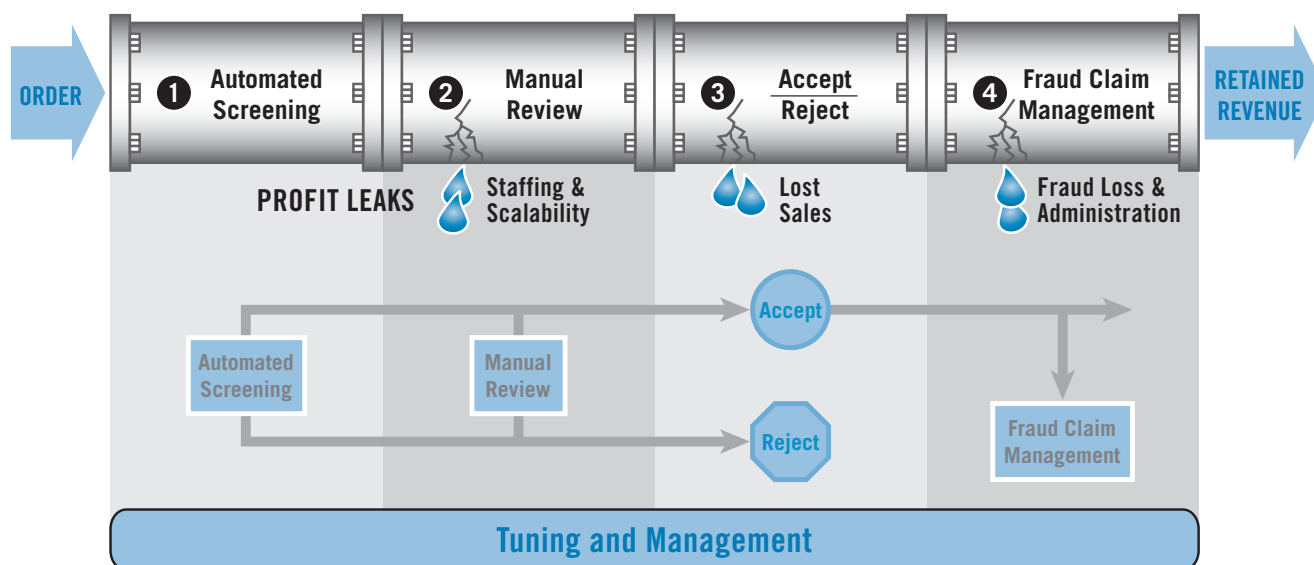
management efficiency in excess of 20% may well be required for healthy online business growth.

Businesses that focus only on managing chargebacks are not seeing the complete financial picture. Online payment fraud impacts profits from online sales in multiple ways. Besides direct revenue losses, 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.

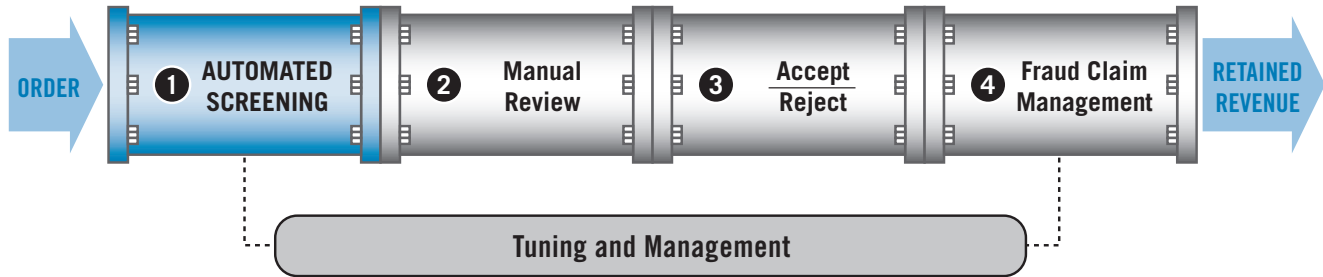
Merchants can gain efficiency by taking a total pipeline view of operations and costs. While the fraud rate is one metric to monitor (and contain within industry and association limits), an end-to-end view is required to arrive at the best possible financial outcome.

In 2005, these “profit leaks” in the Risk Management Pipeline™ impact as much as 28+% of orders for medium merchants and as much as 19+% of orders for larger merchants—restricting profits, operating efficiency and business scalability. This report details key metrics and practices at each point in the pipeline, by company size, to provide merchants with benchmarks and insights that will help them evaluate their own operations. Merchants desiring specific industry cuts of these benchmarks and practices are invited to contact CyberSource for a custom view of pipeline metrics. See end of report for contact information.

## Risk Management Pipeline™



# Stage 1: Automated Screening



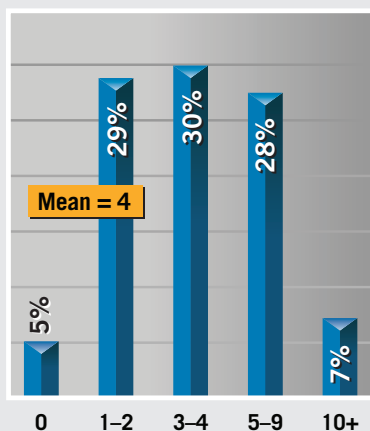
## Fraud Detection Tools

We define detection tools as those used to identify the probability of risk associated with a transaction or validate the identity of the purchaser. Results of tests carried out by detection tools are then interpreted by humans or rules systems to ultimately 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 2005, nearly two-thirds of merchants reported using three or more fraud detection tools, with four tools being the average. Larger merchants dealing with higher order volumes reported using, on average, six tools.

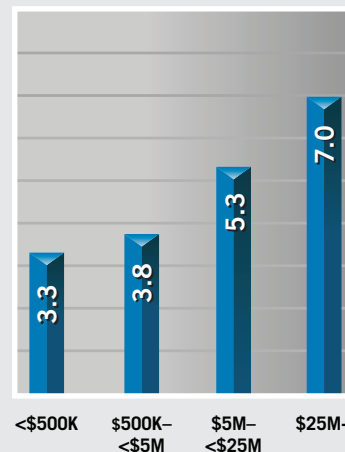
The most popular tools used to assess online fraud risk are shown in chart #3 (see page 6) which shows the current and planned adoption of different tools. Note that the tool usage profile for merchants over \$25M in online sales is different than the overall average, exemplified by higher use of company-specific risk scoring models, negative and positive lists, and sophisticated order velocity monitoring tools.

As in past years, the use of basic fraud detection tools has continued to increase in 2005. The tool most often mentioned by merchants is the Address Verification Service (known as 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.

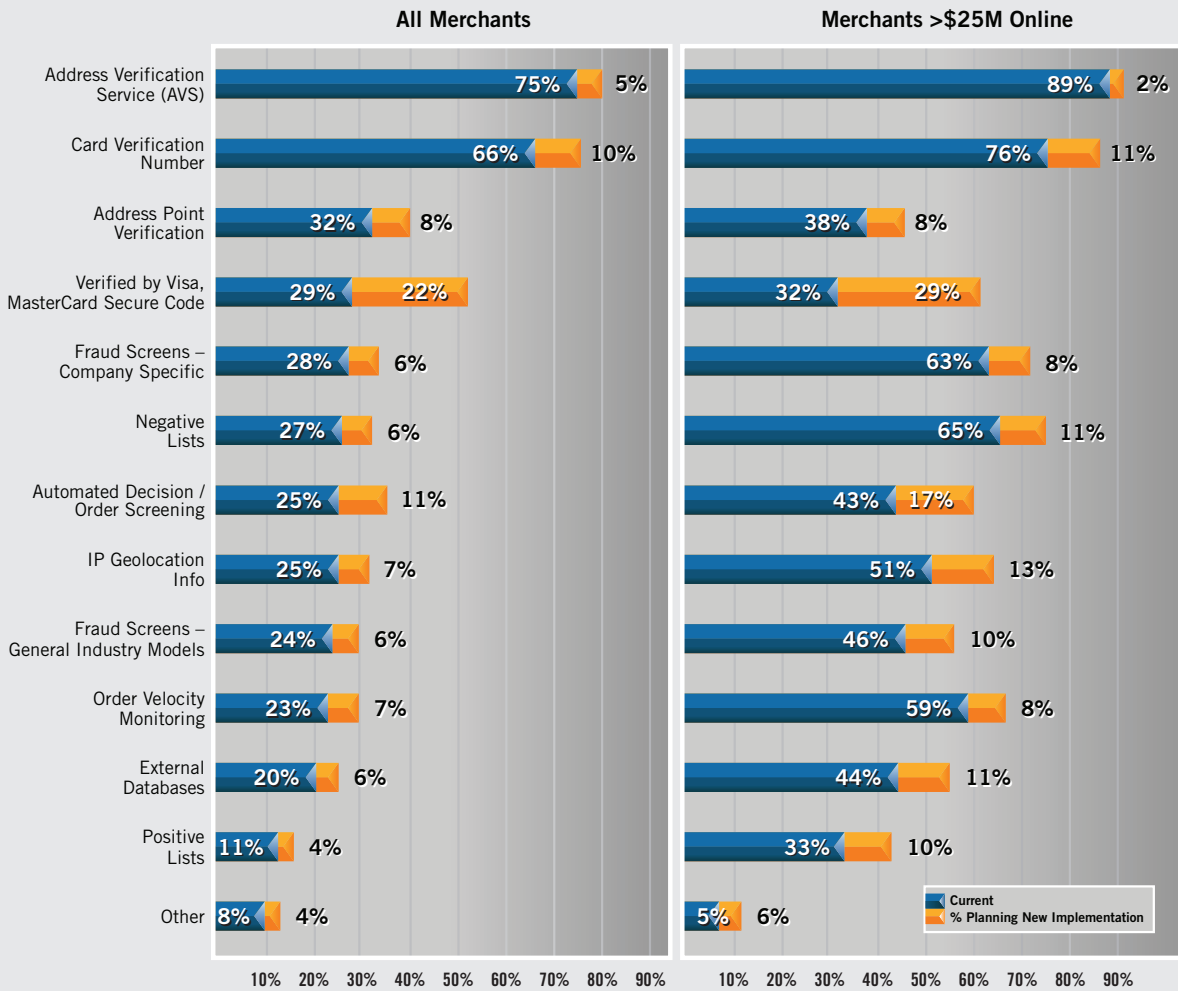
Number of Fraud Detection Tools Used (all merchants)



Number of Fraud Detection Tools Used (by merchant size)



### Fraud Detection Tool Usage



AVS is subject to a significant rate of “false positives” which may lead to rejecting valid orders<sup>2</sup> 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 up-to-date 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.

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 card in their possession in order to provide the additional security digits. Requesting the card verification number during an online purchase can add a measure of security to the transaction. However, these 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 66% today. It appears that asking for the Card Verification Number has become standard practice for many online merchants in 2005.

<sup>2</sup> CyberSource analyzed 12.9 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 AVS “no match” they would incorrectly reject 25% of the good orders and fail to detect 61% of the fraudulent orders.

## Planned 2006 Fraud Tool Use

### Payer Authentication Services Cited As Tool Most Often Planned For Implementation in 2006

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 adoption of payer authentication systems, rising from 19% in 2003 to 29% in 2005. 22% of respondents say they are interested in deploying these systems in 2006 as a new tool to detect and manage fraud. In some cases, implementing these systems can eliminate or 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). If merchants have a sufficiently high direct fraud loss rate, however, 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 Order Screening Figures Prominently In Planned Enhancements

The second "most likely to be implemented" tool is automated order decisioning / screening. These tools help merchants automate order screening by applying a merchant's business rules in the real-time evaluation of incoming orders to detect the probability of fraud. In the current survey 11% of merchants say they plan to add this capability in 2006. However for large merchants (more than \$25 million in annual online revenues) this rises to 17%, most likely due to their need for increased automation.

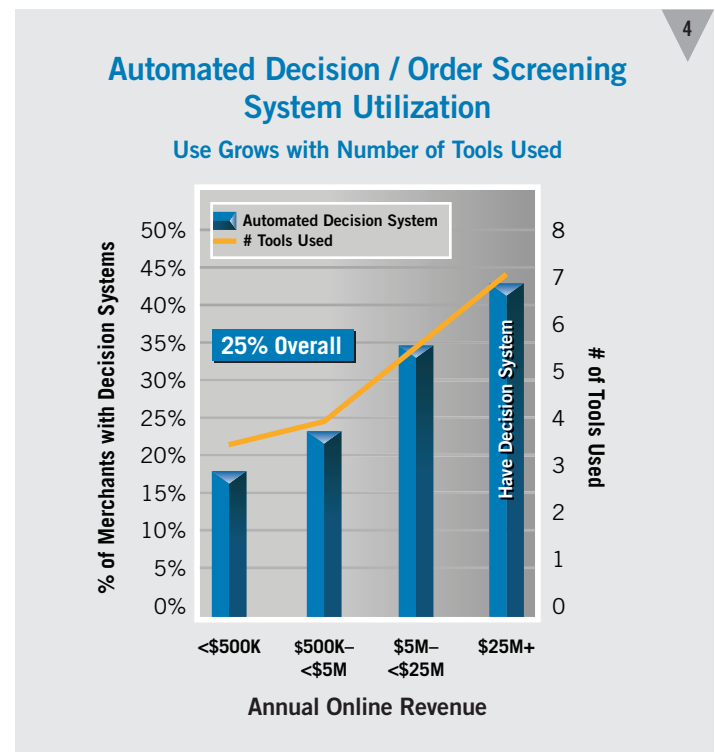
## Automated Decision/Rules Systems

Decision and rules systems provide the basis for automating the evaluation of test results generated by fraud detection tools and determining whether the transaction should be accepted, rejected, or suspended for review. As the number of tools used grows, it is becoming increasingly important for merchants to employ automated systems to interpret and weigh the multiple results for each product

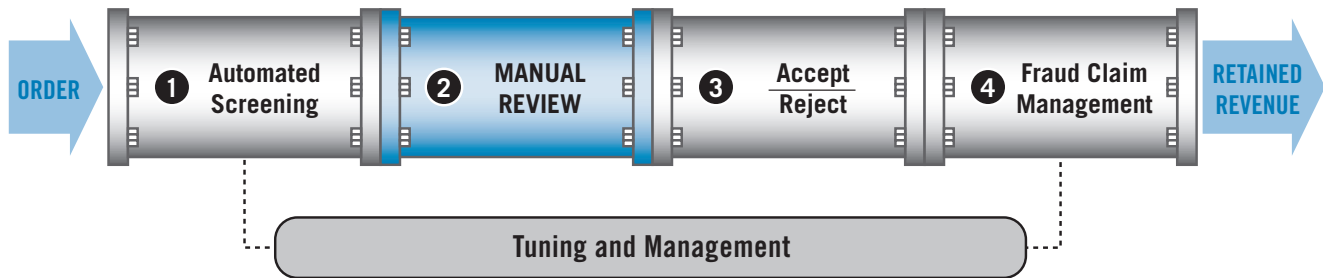
or transaction profile (versus a "one size fits all" screen) to optimize business results. Because fraud patterns are dynamic, and the introduction of new products or services often requires a unique set of acceptance rules, it is imperative that these systems can also quickly adapt to the changing environment. Chart #4 shows that medium and large online merchants tend to employ more automated tools. This is driven largely by the higher volume of orders they have to evaluate. Decision system utilization also appears to correlate with the number of tools employed.

### 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. Manual review is expensive, limits scalability and impacts customer satisfaction. While the rate of manual review was relatively stable in 2005, few merchants cite having budget available to increase review staff now or in the next twelve months. In the face of continued sales growth and cost pressure, this situation presents significant challenges to 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 total online sales increases.

## Manual Order Review Rates

In what should be a highly automated sales environment, 73% of merchants are manually checking orders today. Of the merchants engaged in review, the average rate of manual review exceeds 1 out of 3 orders, and increased from 34% to 35% in 2005. Projecting this rate across all merchants and orders, approximately 26% of all online orders (about one in four) were reviewed in 2005, as compared to 16% in 2000 (approximately one in six orders).

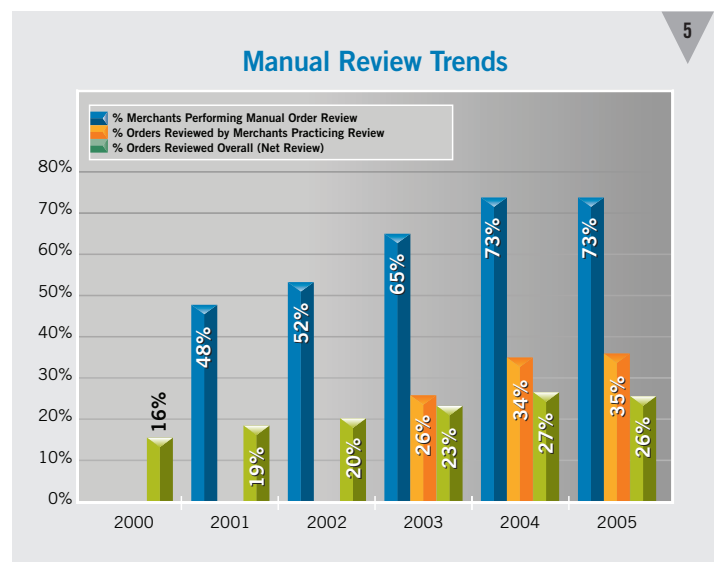
Merchants of all sizes use manual review to manage payment fraud. Chart #6 (see page 9) shows smaller merchants review a higher percentage of orders (perhaps because lower order volumes permit such practice) but even larger merchants review a significant percentage of online orders—and likely devote more resources to this task than is operationally scalable.

While the percentage of online orders being manually reviewed was up slightly in 2005 for those merchants

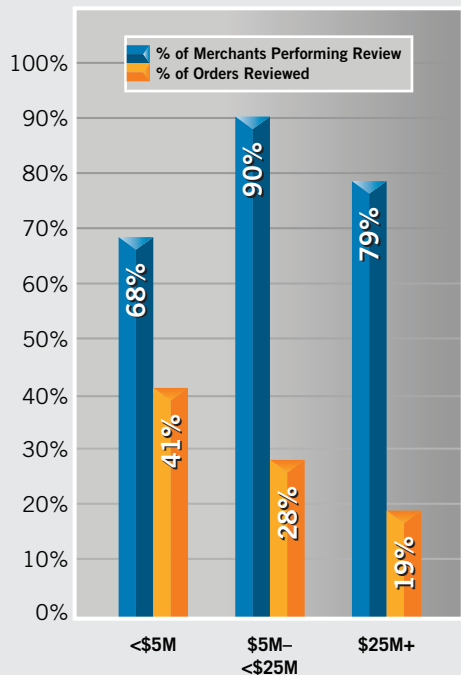
doing manual review, the volume of online sales is up (according to most sources) by 20% or more. As a result, merchants have to manually investigate many more orders in 2005 than they did in 2004. Virtually all online sales forecasts continue to project high growth rates over the next few years. As 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; or 4) improve their methods of identifying riskier orders for review and make the review process itself more efficient.

## Manual Order Review Efficiency

In 2005, survey data shows that 63% of companies review less than 20 orders per hour per reviewer. On average, larger merchants cite being able to review more orders per hour than smaller merchants. This difference may be attributed



### Manual Review by Merchant Size 2005 (For Merchants Engaged in Review)



to a higher utilization of case management systems among larger merchants. 22% of merchants over \$25 million in annual online sales report use of case management systems, nearly three times the overall rate of 8%.

### 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 inconveniencing the customer. Merchants report that 44% of orders reviewed require contacting the customer, 29% require contacting the customer’s bank, and 18% of the orders require 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

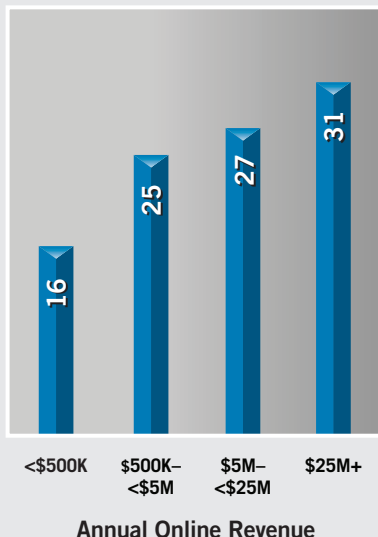
Automated screening and manual order review ultimately result in order acceptance or rejection. A relatively high percentage of orders reviewed are ultimately accepted (see next section)—further signaling opportunities for merchants to improve automated screening and reduce the need for review. A look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

### # Orders Reviewed Per Hour/Reviewer (by Review Rate)

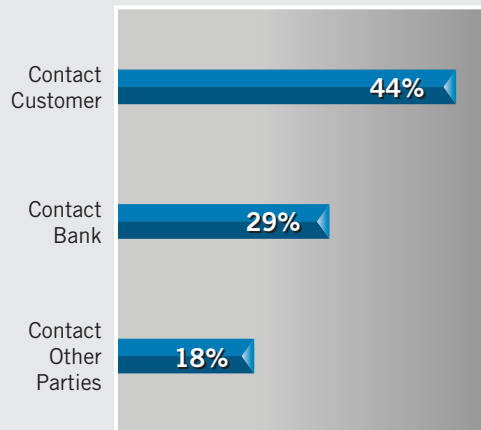
# orders	% of Merchants
<10	34%
10 – 19	29%
20 – 49	20%
50+	17%

Base: Those who manually review to screen for online fraud  
n = 293

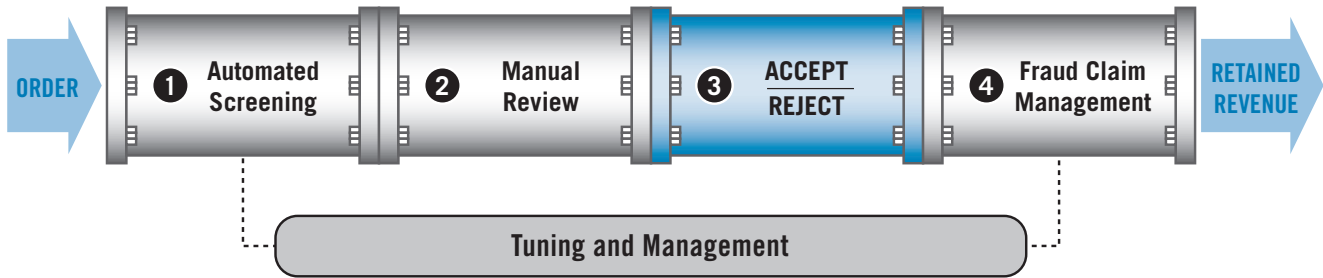
### # Orders Reviewed Per Hour/Reviewer (by Merchant Size)



### Actions Taken During Order Review (% of orders requiring)

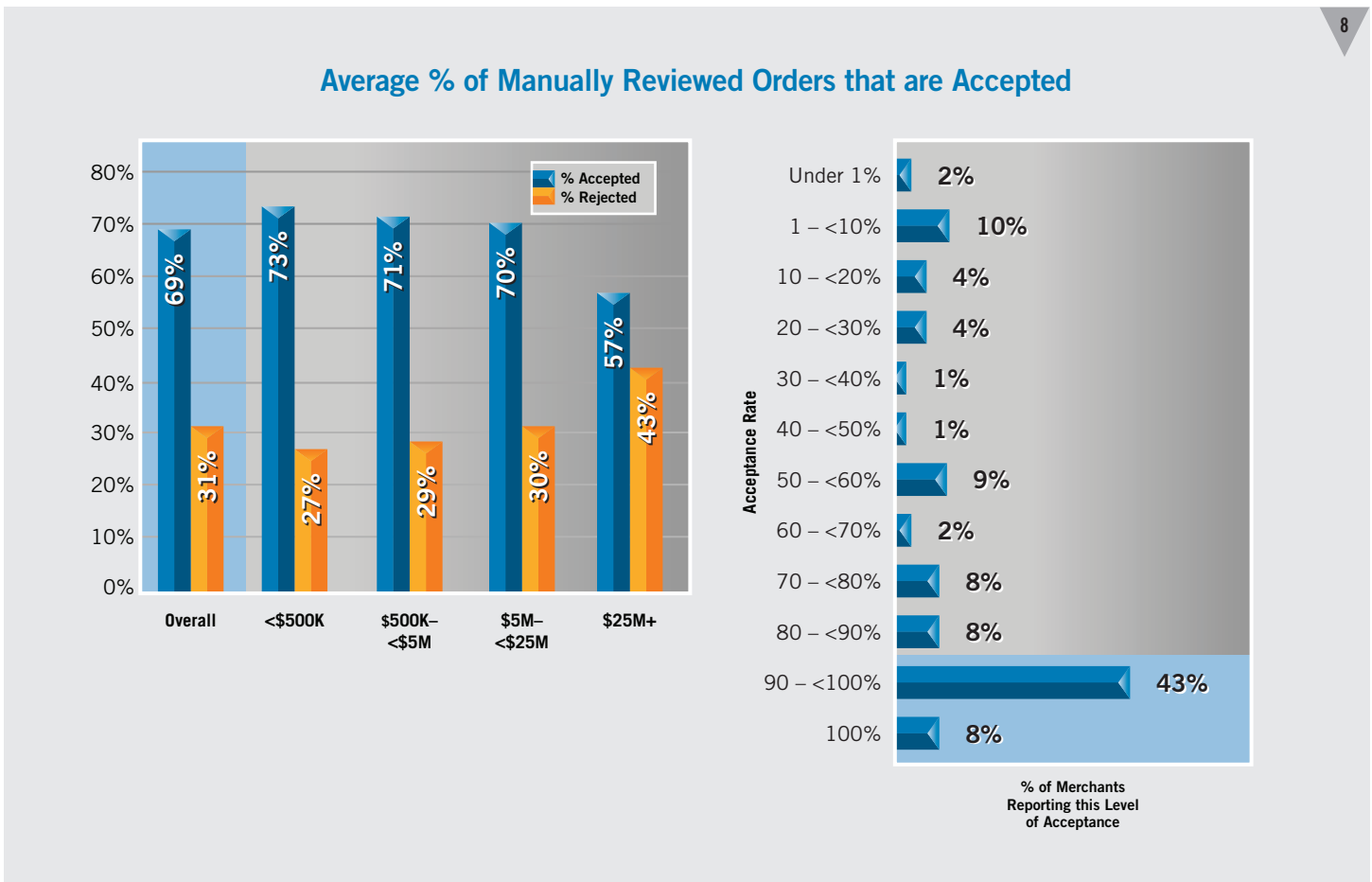


# Stage 3: Order Dispositioning (Accept/Reject)



## Post-Review Order Acceptance Rates

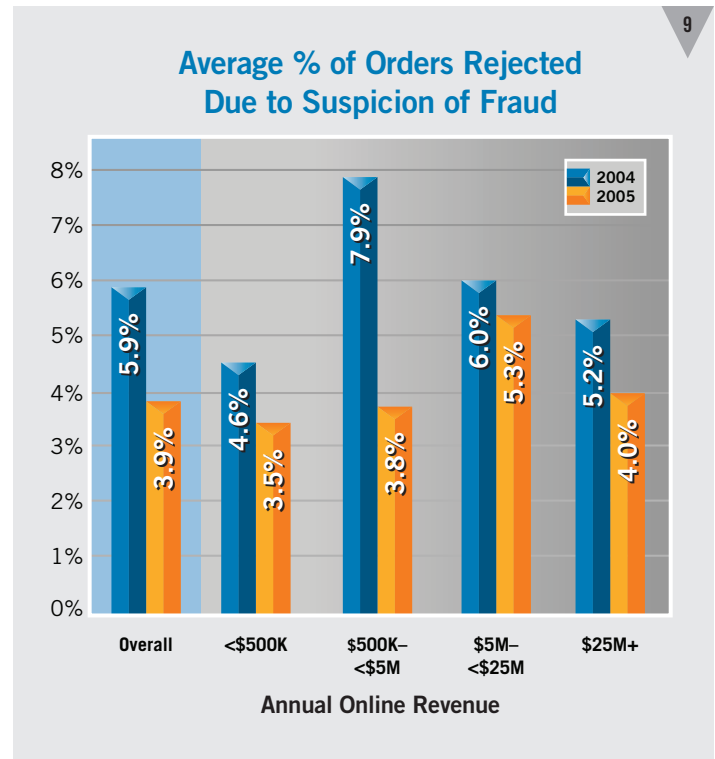
In 2005, merchants surveyed indicated that they ultimately accepted over two-thirds of the orders they manually reviewed (see chart #8). Over 50% of merchants report they accept 90% or more of orders they manually review.



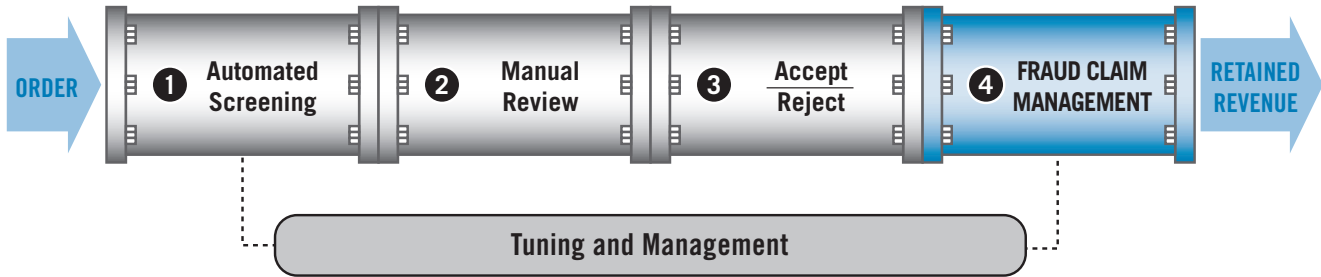
## Overall Order Rejection Rates

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 2005, merchants participating in the survey reported a drop of 2 percentage points in their order rejection rates from 5.9% in 2004 to 3.9%. Yet for every fraudulent order they received they rejected almost 4 orders due to suspicion of fraud.

Larger online merchants, who saw a 0.3% increase in their accepted fraud rate, more than made-up for the additional fraud loss with a 1.2% drop in order rejection. The net impact: they were able to increase valid order acceptance, and therefore total sales by almost 1%. This demonstrates the trade-off between potentially rejecting valid orders and associated incremental revenues in order to minimize fraudulent order losses. Sophisticated merchants realize that 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.



# Stage 4: Fraud Claim Management

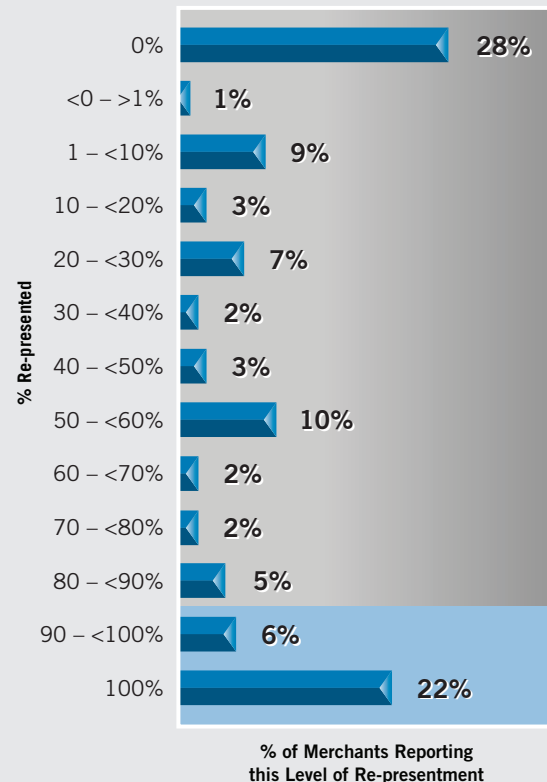
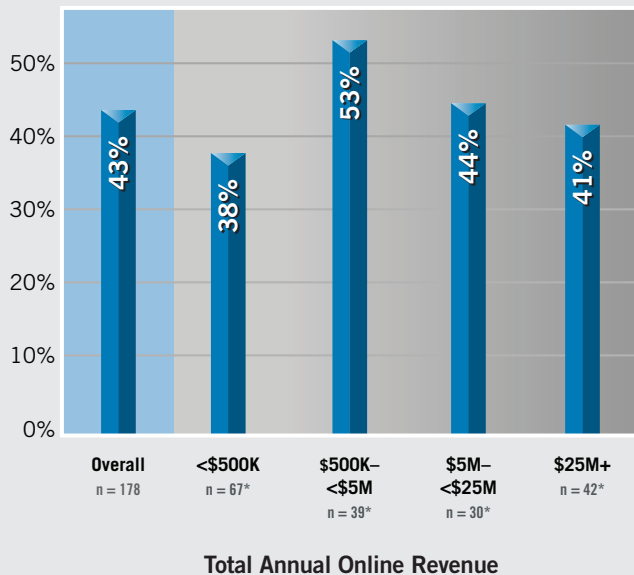


## Fighting Chargebacks

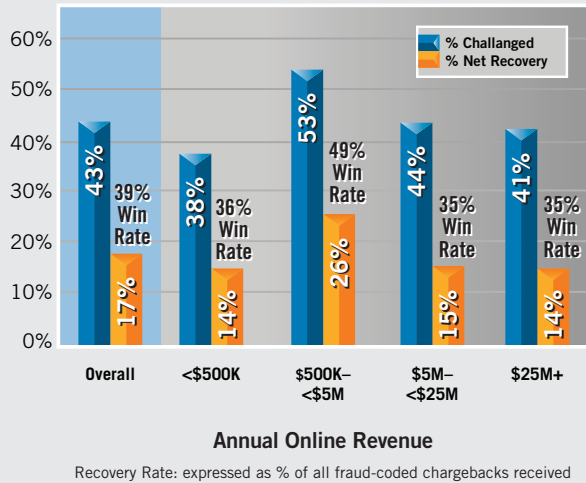
This year's survey examined practices associated with reviewing and contesting chargebacks ("re-presentation").

Overall, an average of 43% of fraud-coded chargebacks are re-presented, with over one-in-four merchants contesting 90-100% of chargebacks and a nearly equal amount not contesting any (see chart below).

### Average % Total Fraud-Coded Chargebacks Re-presented



### Fraud Chargeback Re-resentation: Win Rate/Net Recovery Rate (Overall and by Merchant Size)



## 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). Considering the financial impact of both fraud claim routes (chargebacks and credit issuance) merchants may wish to 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.

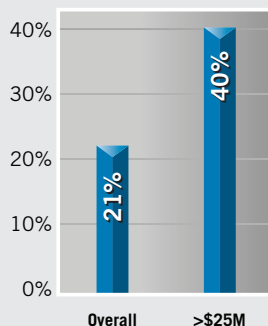
Merchants report that they win, on average, 39% of the chargebacks they dispute. This translates to an overall net recovery rate of 17% (meaning 17% of all fraud-coded chargebacks are recovered). Clearly, having an efficient re-resentation process and understanding what can be done to recover a higher percentage of chargebacks can help enhance profitability and reduce fraud loss.

## Chargeback Management Tools

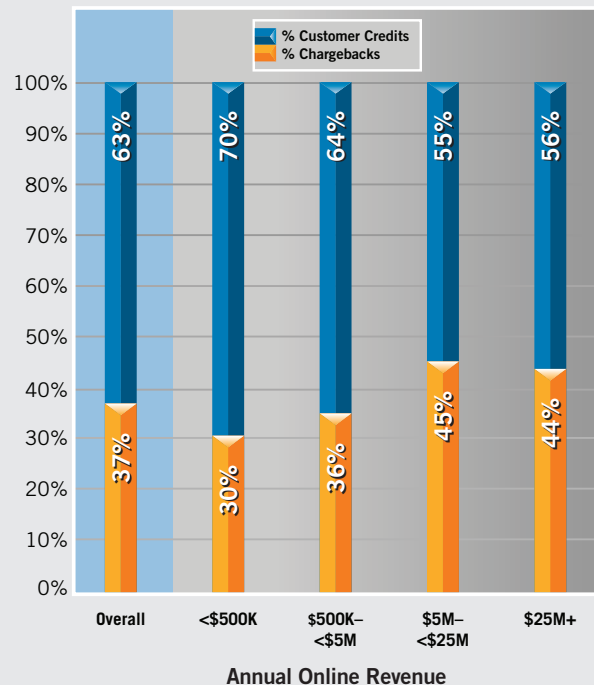
Of course disputing chargebacks is not an easy or cost-free process. Merchants must manage and organize all order, delivery and payment information to successfully dispute

fraudulent orders with financial institutions. Merchants are beginning to adopt automated systems for handling this aspect of the pipeline. As chart #12 shows, larger merchants, managing higher volumes of fraudulent orders, tend to invest in automated re-resentation tools more than the average online merchant.

### Chargeback Management & Re-resentation Tools (percent of merchants using)



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

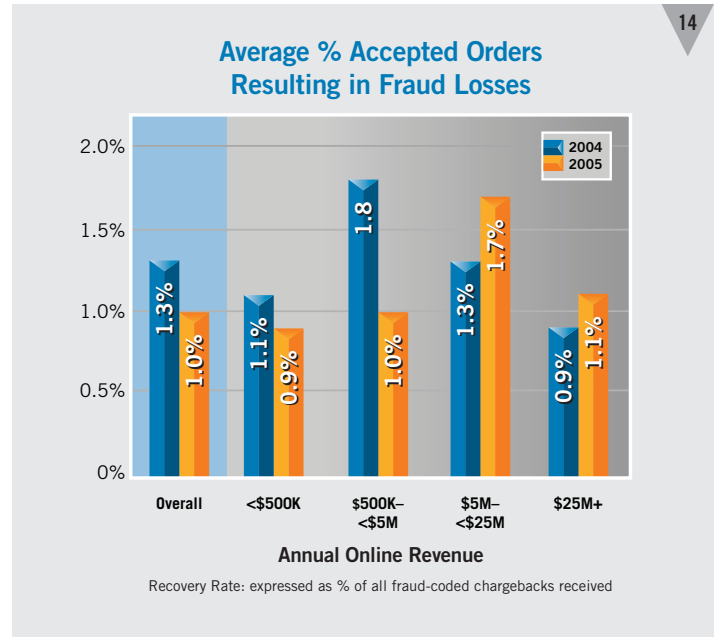
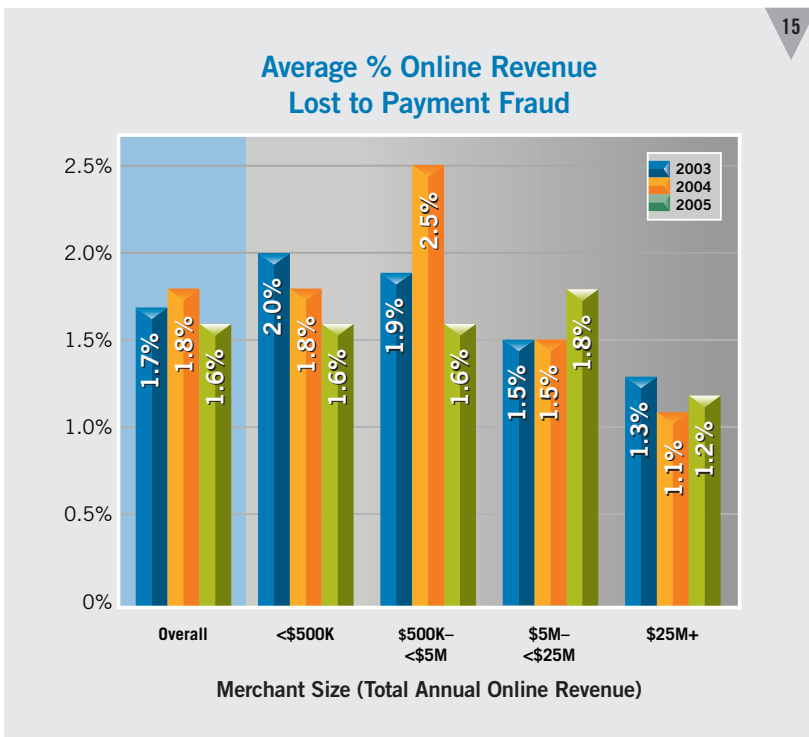


## Fraud Rate Metrics

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. Therefore 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.

### 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.

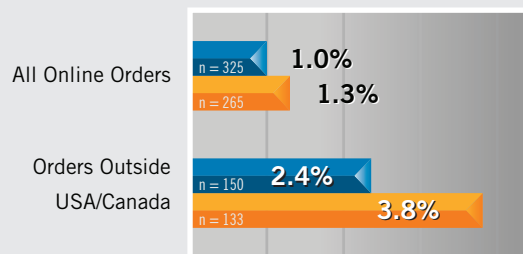
### Fraudulent Order Rate for Accepted Orders

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. The loss trend between 2004 and 2005 is consistent with other related metrics which depict smaller merchants reporting a decline in fraudulent order rates while larger merchants reported an increase. Overall, 21% of merchants report experiencing a fraudulent order rate that exceeds 1%.

### International Orders Carry Higher Risk

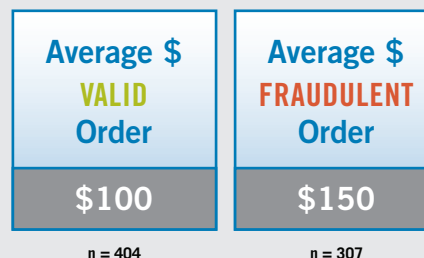
Fifty-five percent of merchants surveyed accepted orders from outside the U.S. & Canada in 2005. International sales accounted for an average of 14% of total orders for these merchants. That same group reported that the actual direct fraud rate on international orders averaged 2.4% or more than twice the overall fraud rate for online orders. While online sales in the U.S. are still growing by 20% or more each year,

### % of Orders Accepted That Turn Out to be Fraudulent



Ratio of International fraud to overall fraud 2.4:1 in 2004

### Value of a Fraudulent Order

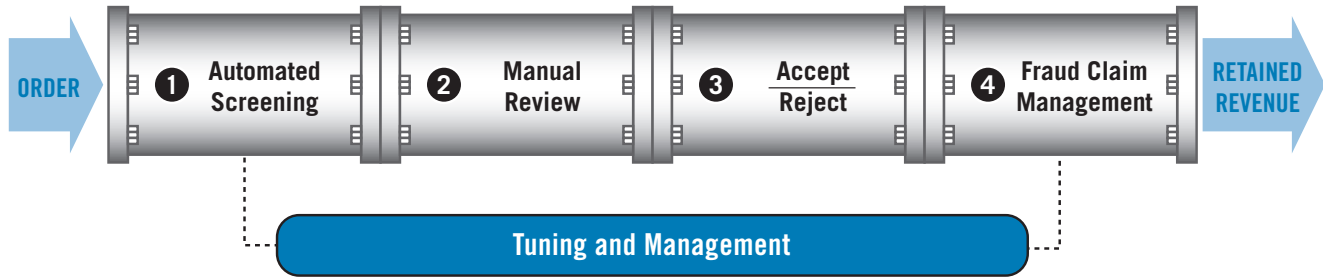


sales in Europe and many other markets are showing even higher growth. Though international markets represent an attractive opportunity, online merchants must make sure that their fraud detection and management systems are robust enough to handle the additional risk involved. Merchants who sell online 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 overall average rate of 3.9% and is approximately 1 out of every 8 international orders received.

### Average Value of Fraudulent Order is 1.5 Times Higher than a Valid Order

The median value of a fraudulent order in the survey was \$150 or 50% higher than the \$100 median value of a valid order. 2005 median order values were the same as those reported in 2004

# Tuning & Management

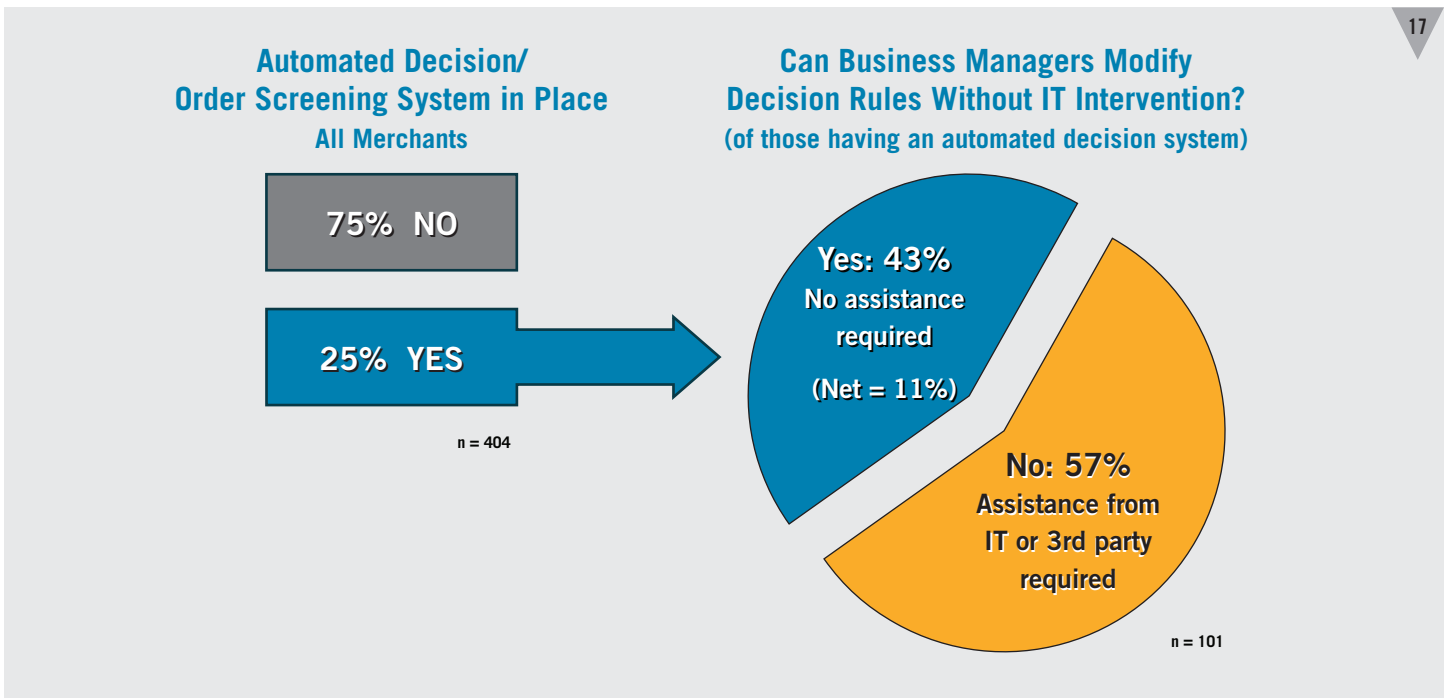


## Maintaining and Tuning Screening Rules

Among merchants having an automated order screening system in place, only 43% have systems that allow business managers to modify decision rules without assistance from internal IT staff or external third parties (meaning overall, only 11% 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? Fifty-one percent of merchants spend more than 0.5% of their online revenues to manage online payment fraud while 49% spend less than 0.5%. The median ratio of fraud management expense to sales is 0.5% across all merchants, although some 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 staff). 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 #18 on next page.)

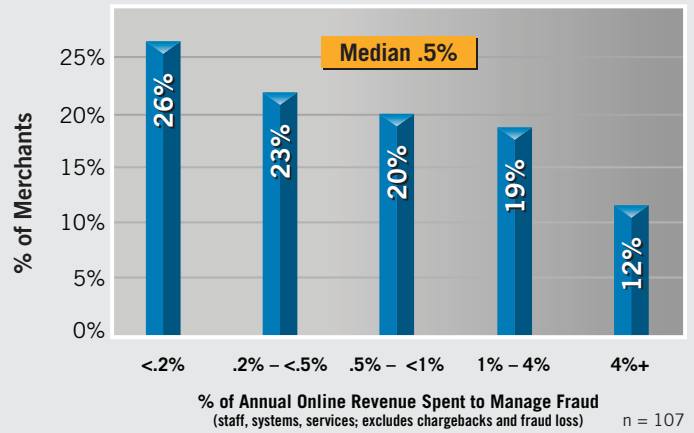


## Budget Allocation

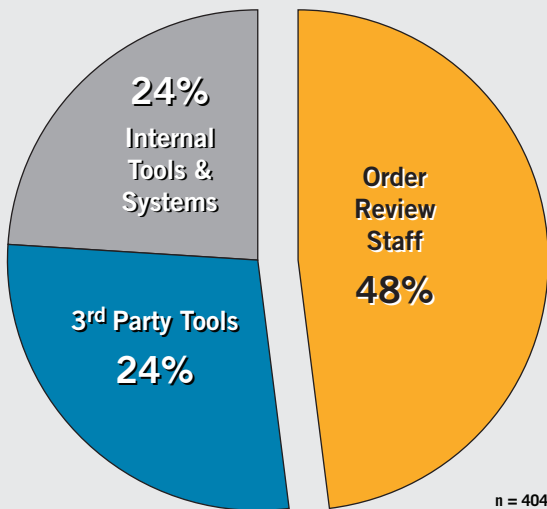
On average, order review staff costs consume 48% of the fraud mitigation budget (see chart #19). The remainder is allocated as follows: 28% for third party tools or services and 24% on internally developed tools and systems. Clearly, review staff costs are the dominant factor, and only 22% of merchants cite plans to increase review staffing in 2006. 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.

### How Much Merchants Spend Annually on Fraud Management

(percent of merchants operating at defined expense level)



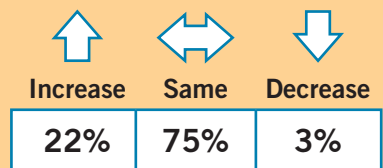
### Average % Spending Allocation for Fraud Management



### Review Staffing

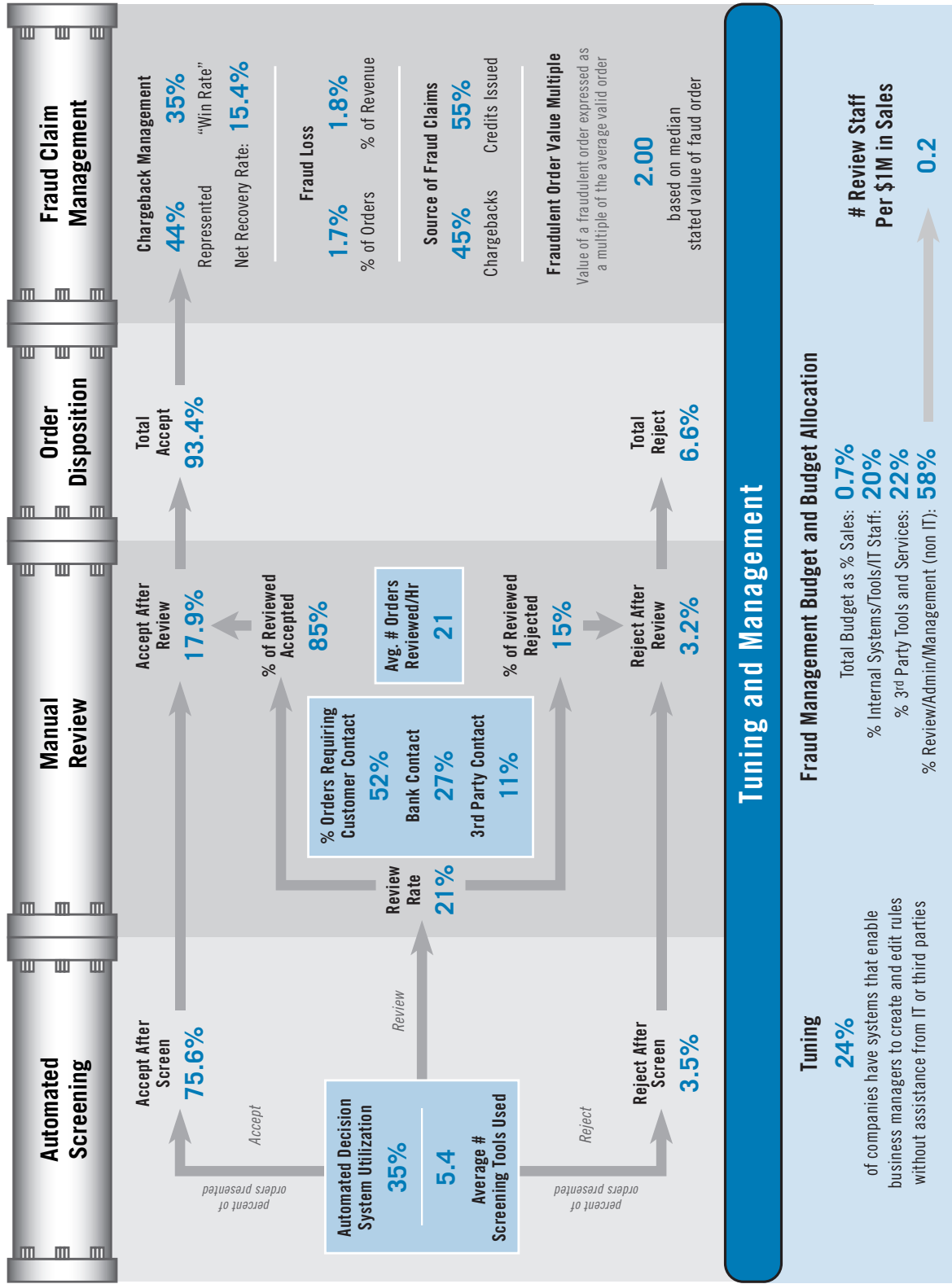
# Full-Time Review Staff	Average Annual Online Revenue	Annual Revenue Per Reviewer
1	\$220K	\$229K
2	\$1 Mil	\$500K
3 - 4	\$2 Mil	\$570K
5 - 9	\$34 Mil	\$4.9 M
10+	\$35 Mil	<\$3.5 M

Planned Staffing Levels for 2006



Base: Those with 1 or more full-time manual review staff n = 288

# 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](http://www.cybersource.com/contact_us)

© 2005 CyberSource Corporation. All rights reserved. The Risk Management Pipeline is a trademark of CyberSource Corporation.

©2006 CyberSource Corporation. All rights reserved.

# 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](http://www.cybersource.com). For sales assistance phone: 1-888-330-2300; or e-mail: [sales@cybersource.com](mailto:sales@cybersource.com)

## CyberSource Risk Management Solutions

Our suite of modular, scalable services—ranging from fully managed services to individual tools—has helped thousands of companies achieve superior results in managing online fraud. Survey results show that merchants using CyberSource solutions manually review fewer orders, reject fewer orders and achieve exemplary fraud control. Our solutions can be quickly and easily implemented as a single component or as fully-integrated systems, and can be managed in-house, outsourced or constructed as a blend of both.

### Managed Risk Service

This service provides analysis, design, modeling and monitoring services that will help optimize your sales conversion while minimizing manual review and fraud risk. We'll collaborate with you to set business metrics, review performance, and provide easy-to-use business tools that let you control as little or as much as you wish. The service starts with a complete analysis of your company's transaction history and business processes, and ensures installation of a fully tailored solution with ongoing monitoring and tuning to further enhance business results.

### Rule & Decisioning Systems: CyberSource Decision Manager

CyberSource offers a full range of decision management systems ranging from hosted solutions that include custom rule and case management capabilities (CyberSource Decision Manager Standard and Advanced Editions) to locally managed software which can be customized for your particular application (CyberSource Decision Manager Custom Edition). These systems employ our exclusive risk scoring service (CyberSource Advanced Fraud Screen enhanced by Visa—see below) as well as other external services; and, based on your business rules, automatically tag the order as “accept”, “reject”, or “review”.

### Fraud Detection/Verification Tools

- **Risk Scoring Service: CyberSource Advanced Fraud Screen enhanced by Visa**  
The only risk scoring service endorsed by Visa. CyberSource Advanced Fraud Screen enhanced by Visa (AFS) provides a real-time payment card fraud risk assessment. AFS relies on a patented process that blends multiple risk models and assesses over 150 attributes of the transaction to determine the fraud risk associated with the order, all in less than 2 seconds. CyberSource and VISA co-developed the system, and engage in closed-loop modeling to maximize fraud detection and minimize false-positives. The results from AFS include a numerical risk score as well as risk profile codes indicating the type or types of risk detected by the system.
- **Payer Authentication Services: Verified by Visa, MasterCard SecureCode**  
Our convenient, hassle-free, 3D Secure™ compliant payer authentication service gives consumers and merchants the online payment card security promise offered by Visa (Verified by Visa) and MasterCard (SecureCode)—all with the ease of a single connection to CyberSource.
- **Delivery Address Verification & Distribution Compliance**  
CyberSource offers Delivery Address Verification (DAV) services to verify the validity of addresses worldwide and comply with USPS requirements such as bar code and carrier route identification. If an address is in error and is found to be correctable, DAV will return a corrected address and identify address elements in error. Our Export service helps merchants comply with U.S. Government Bureau of Export Administration (BXA) procedures involving denied party and denied country checking, as well as internal company policies.

## CyberSource Payment Solutions

CyberSource offers complete domestic and global payment processing services in multiple currencies, including credit and debit cards, electronic checks, Bill Me Later, PayPal, CheckFree, regional payment cards, bank transfers, direct debit, and subscription payments.

# About CyberSource

---

CyberSource Corporation is a leading provider of electronic payment and risk management 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. Approximately 12,000 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 full pipeline process analysis is provided in the Appendix of this report. 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](http://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](http://www.cybersource.com/contact_us)**
- **Risk Management Solutions: visit [www.cybersource.com/risksolutions](http://www.cybersource.com/risksolutions)**
- **Global Payment Solutions: visit [www.cybersource.com](http://www.cybersource.com)**

## For More Information

- Call **1.888.330.2300**
- Email **[info@cybersource.com](mailto:info@cybersource.com)**
- Visit **[www.cybersource.com](http://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](mailto:info@cybersource.com)

### Europe

CyberSource Ltd.  
400 Thames Valley Park Drive  
Thames Valley Park  
Reading RG6 1PT  
United Kingdom  
T: +44 (0) 118.965.3819  
F: +44 (0) 870.460.1931  
Email: [uk@cybersource.com](mailto:uk@cybersource.com)

### 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](mailto:mail@cybersource.co.jp)