



5th Annual **ONLINE FRAUD REPORT**

Credit Card Fraud Trends and Merchants' Response

2004 Edition

Sponsored by CyberSource Corporation

Conducted by Mindwave Research

Methodology

Merchants who participated in this survey reflect a blend of small-, medium-, and large-sized businesses based in North America. They represent companies in their first year of online sales to the largest e-retailers in the world. The mix of merchants (by size of online revenues) who participated in 2003 was nearly identical to those who participated in 2002. Predictably, however, participating merchants had more years of experience selling online in 2003.

The survey was conducted via an online questionnaire at the MindWave Research website — 333 merchants completed the survey between October 14th and October 21st, 2003. 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
Total number of merchants participating	341	333

Annual Online Revenue

Less than \$500K	28%	29%
\$500K to Less than \$10M	44%	43%
Over \$10M	28%	28%

Duration of Online Selling

Less than One Year	12%	10%
1-2 Years	28%	19%
3 or More Years	60%	71%

Risk Management Responsibility

Ultimately Responsible	32%	49%
Influence Decision	68%	51%

Table of Contents

Methodology	2
Executive Summary	4
Key Findings & Analysis	4
Conclusions	5
Business Impact of Online Fraud in 2003	6
Online Fraud Revenue Loss Rate Declines	6
International Fraud Rate Four Times Higher	7
Order Rejection Rate Three Times Higher Than Fraud Rate	7
Negative Impact on Staff Time and Bottom Line	8
More Merchants Report Online Fraud is a Serious Business Issue	9
Common Practices for Managing Online Fraud in 2003	10
Fraud-Prevention Efforts Increase	10
Manual Intervention Efforts Continue to Increase	11
Plans For Managing Online Fraud in 2004	14
Most Merchants Expect Fraud-Control Costs to Increase	14
Conclusion	15
Resources	16
CyberSource Risk Management Solutions	16
About CyberSource	17

List of Figures

Chart 1. Online Fraud Casts a Large Shadow	5
Chart 2. Online Fraud Rate Declines as % of Online Revenue	6
Chart 3. % Accepted Orders Later Determined Fraudulent	6
Chart 4. % Orders Declined/Accepted Due to Fraud.....	7
Chart 5. Negative Impact of Online Fraud.....	8
Chart 6. % Reporting Fraud as a Serious Business Issue	9
Chart 7. Fraud Management Methods.....	10
Chart 8. Use of Manual Review	11
Chart 9. Manual Review Use by Online Revenue Size	11
Chart 10. % of Manually Reviewed Orders Ultimately Accepted.....	12
Chart 11. Manual Review Techniques.....	13
Chart 12. 2004 Fraud Management Cost Expectation.....	14
Chart 13. Planned Fraud Management Methods for 2004.....	14
Chart 14. Adoption of Visa and MasterCard Payer Authentication	15

Executive Summary

Managing online credit card fraud continues to be a major challenge for merchants of all sizes. To better understand this challenge, CyberSource sponsors annual surveys addressing the detection, prevention and management of online fraud. This report summarizes key issues and trends identified in the fifth annual survey. The survey was conducted by Mindwave Research, an independent market research company. Survey focus areas included:

- Online fraud's impact on business
- Merchant efforts to manage fraud
- Plans to combat online fraud in the future

Key Findings & Analysis

The results of the fifth annual survey (conducted in October, 2003) indicate that merchants selling online are doing a better job at controlling the direct costs of online fraud. However the indirect, hidden costs of fraud are becoming an even larger problem. Two-thirds of merchants report that online credit card fraud is a serious business issue in 2003. Almost half expect the costs of managing and controlling online fraud will increase in 2004, while only 7% expect those costs to decrease.

Revenue and Direct Fraud Losses

Over the past four years, the estimated revenue loss due to online credit card fraud has declined from 3.6% of total online revenues in 2000, to 1.7% in 2003. As U.S. business-to-consumer online sales are expected to approach \$100 billion in 2003, total online revenues lost to fraud are likely to exceed \$1.6 billion for the year. Merchants also reported that direct credit card fraud losses (bank chargebacks and credits issued directly to consumers to avoid fraud chargebacks) averaged 1% of orders in 2003. In addition, the survey shows that direct fraud-loss rates for orders originating outside the U.S. and Canada is four times higher than U.S. and Canadian orders.

Rejecting Orders Due to Suspicion of Fraud

For every accepted order which results in a fraud chargeback or customer fraud claim, merchants reject more than 3 additional orders. Merchants whose direct fraud-loss rate is above 1% are turning away twice as many orders on average (nearly 8%). For merchants accepting orders originating outside of the U.S. and Canada, the rejection rate is almost 8% as well. It is virtually certain that some of these rejected orders are valid, but in the attempt to reduce direct fraud losses, merchants reject orders that appear suspicious. The fact that on average, merchants ultimately accept two-thirds of orders they manually screen, seems to indicate that the proportion of valid orders they reject is significant.

Use of Anti-Fraud Tools

More merchants are using basic fraud protection techniques, including manual review, the address verification service (AVS), and card verification number (CVN) checks. There is an increase in the use of new payer authentication programs offered by Visa and MasterCard. These programs require a credit card user to enter a password during the checkout process to authenticate the transaction (making it more difficult for lost or stolen cards to be used for online purchases). Implementation of cardholder association payer authentication systems can protect merchants from chargebacks due to fraud, but this protection only applies if a merchant can maintain chargeback order rates below thresholds set by the card associations (typically 1%).

Increased Reliance on Manual Review

Employee intervention to detect and prevent fraud increased significantly in 2003. The percentage of merchants employing manual review methods reached 65%, compared to just over half in 2002. Manual order review continues to be the second-most-popular method for managing online fraud (after the use of AVS during the credit card authorization process). Manual review is being used by 55% of smaller online sellers in the survey, while 72% of merchants doing more than \$25 million in annual online sales employ the practice.

The percentage of orders reviewed manually has been steadily increasing over the past four years. In this survey, the manual review rate increased, on average, from 20% to 23% of online orders. While increasing manual review has helped to reduce direct fraud losses, it may be too costly for merchants to increase staff commensurately as online sales continue to grow 25-30% each year. With online sales growing nearly 30% in 2003, it is likely that the majority of merchants experienced a significant increase in their fraud-control costs due to increased sales and increased reliance on manual review to control fraud losses.

Consumer Cost of Manual Review

Contacting customers by phone or email represent two of the top three manual review techniques that surveyed merchants use to verify orders in 2003. Most manual review processes typically involve re-contacting the customer to validate or collect information. This means that customers are directly inconvenienced as they must provide additional information, and wait longer for order approvals and delivery of products or services. It is likely that increased reliance on manual review will result in lost sales or fewer repeat purchases.

Shifting the Burden of Authentication onto Consumers

When asked what fraud management tools they plan to implement or enhance in 2004, merchants reported that increased use of CVN and new payer authentication systems are the top two actions they plan to take. Both require online shoppers to provide more information during the checkout process to verify their orders.

Conclusions

While merchants appear to be gaining in the battle against direct fraud loss, this progress comes at a high cost—increased manual review and rejection of valid orders. The impact of online fraud casts a larger shadow over profitable online operations than just the visible direct costs of fraud, as measured by credit card chargebacks and credits issued to avoid customer fraud disputes (see Chart 1).



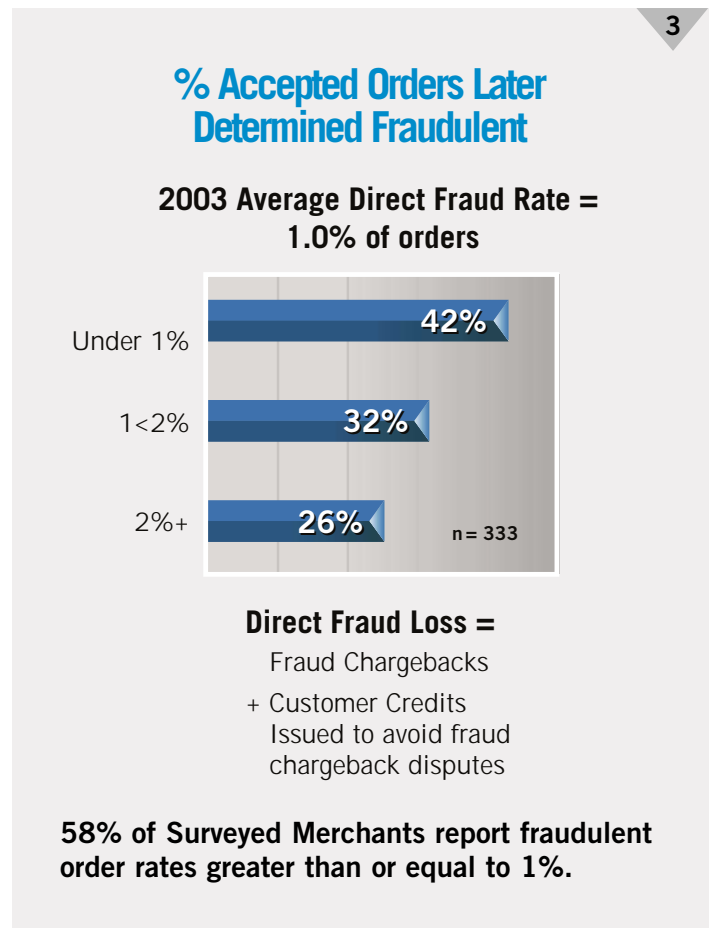
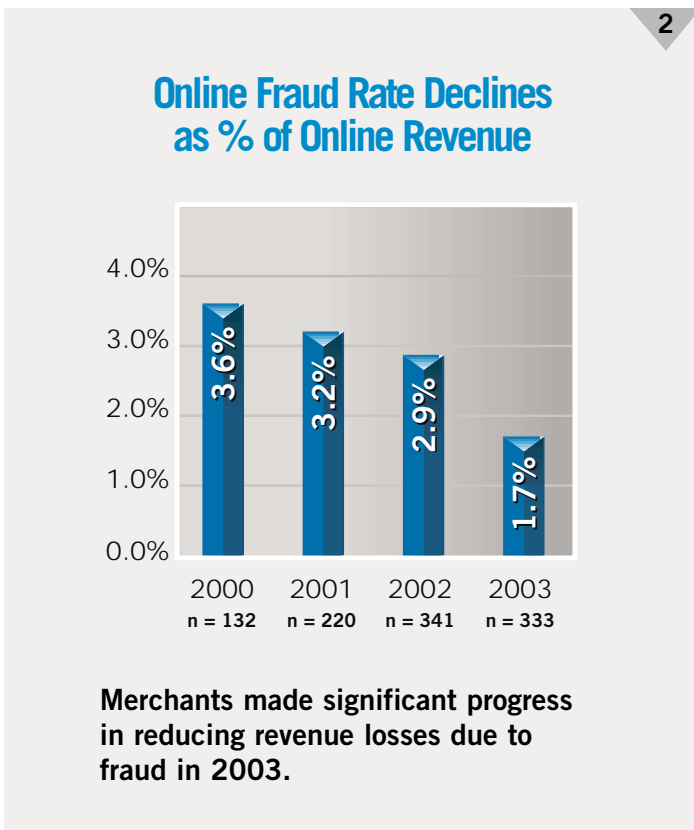
Current merchant approaches of adding staff or rejecting more orders as online order volumes grow are not scaleable, and can reduce sales and profit growth. Merchants are also facing an ever-more-difficult challenge of avoiding chargeback monitoring programs and penalties as card associations continue to make greater demands. Finally, while online sales are growing faster in markets outside North America, that sales potential comes with dramatically greater fraud-management challenges. To maximize online profit growth, successful merchants will need to learn how to apply best practices, employ best technology, and re-engineer order review and acceptance processes to optimize their business while minimizing true fraud costs.

II. Business Impact of Online Fraud in 2003

Online Fraud Revenue Loss Rate Declines

Merchants reported a significant drop in the percent of online revenues they expect to lose to fraud in 2003. The average percent of revenues lost to online credit card fraud is down to 1.7% for the year. We have seen a steady decline in this estimated revenue-loss rate over the past four years (see Chart 2, below).

In 2003, for the first time, we drilled down on the issue of fraud-loss rates. Over the years there has been a wide range of estimates given for online credit card fraud rates. The card associations report the rate to be less than 1%, on average. They also report that the fraud rate for online transactions is 5 – 10 times higher than for face-to-face credit card transactions. However, the card associations only see a portion of the total impact of online fraud —the "direct fraud loss" due to bank chargebacks initiated by cardholders with their issuing credit card banks (claiming that their cards have been charged fraudulently). In some cases, consumers initiate a dispute directly with the merchant, and some merchants will issue customer credits to avoid chargeback fees and penalties. In the current survey, we specifically asked merchants to provide an estimate of their "direct fraud-loss" rate (i.e. fraud chargebacks and any credits issued to customers to avoid fraud chargebacks). The average direct fraud-loss rate found in the survey is 1%, however only 42% of merchants report a direct fraud-loss rate less than 10%, while 58% had a direct fraud-loss rate at or above 1% (see Chart 3 below). On October 1st 2003, Visa implemented new rules for merchants accepting "card not present" transactions, requiring that they keep their chargeback rates to less than 1% and fewer than 100 chargebacks per month¹. Previously, Visa had allowed merchants to have less than 2.5% and less than 50 total chargebacks per month to avoid additional chargeback penalties and possible cancellation of Visa privileges. So it is increasingly important in 2004 for merchants to control their direct fraud-loss rate and chargebacks.



International Fraud Rate Four Times Higher

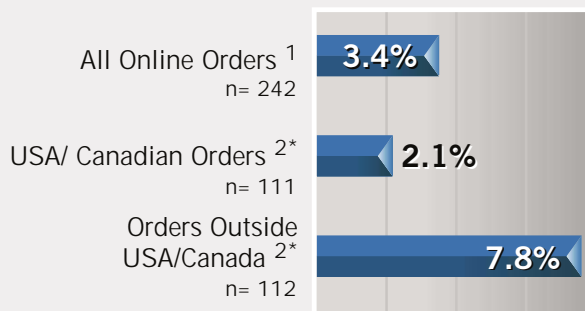
While the new Visa rules will likely have a greater impact on larger online sellers, any merchant accepting orders from outside the U.S. and Canada should consider taking additional measures to control online credit card fraud. Merchants in the survey were asked to provide estimates of their direct fraud-loss rate for orders inside the U.S. and Canada, as well as for orders coming from outside the U.S. and Canada (if they accepted such orders). The direct fraud-loss rate on orders from outside the U.S. and Canada was four times higher than the rate inside the U.S. and Canada (see Chart 4) at 3.2%. Merchants who want to grow their online revenues by accepting orders from other countries must consider carefully how they are going to manage the problem of online credit card fraud cost-effectively.

Order Rejection Rate Three Times Higher Than Direct Fraud Rate

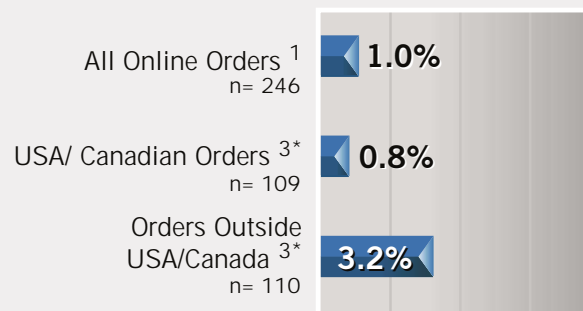
To control direct fraud losses (both for the absolute dollar savings and to avoid card association penalties or cancellation), merchants are rejecting a significant number of orders due to suspicion of fraud. It is likely that some of these orders are valid. On average, for every fraudulent order incurred, merchants reject more than three other orders due to suspicion of fraud (see Chart 4). A similar order-rejection to actual-fraudulent-order ratio is found for orders from outside the U.S. and Canada, but the absolute level of order rejection is much higher, with almost 8% of orders being rejected. Merchants reject orders from outside the U.S. and Canada at a rate almost four times higher than domestic orders, and yet still incur direct fraud losses four times higher than domestic direct fraud losses. Clearly the problem of managing online credit card fraud for sales outside the U.S. and Canada is much more difficult than the already challenging problem of managing domestic fraud.

4

Business Issue % Orders Declined Due to Suspicion of Fraud



% Orders Accepted That Turn Out to be Fraudulent

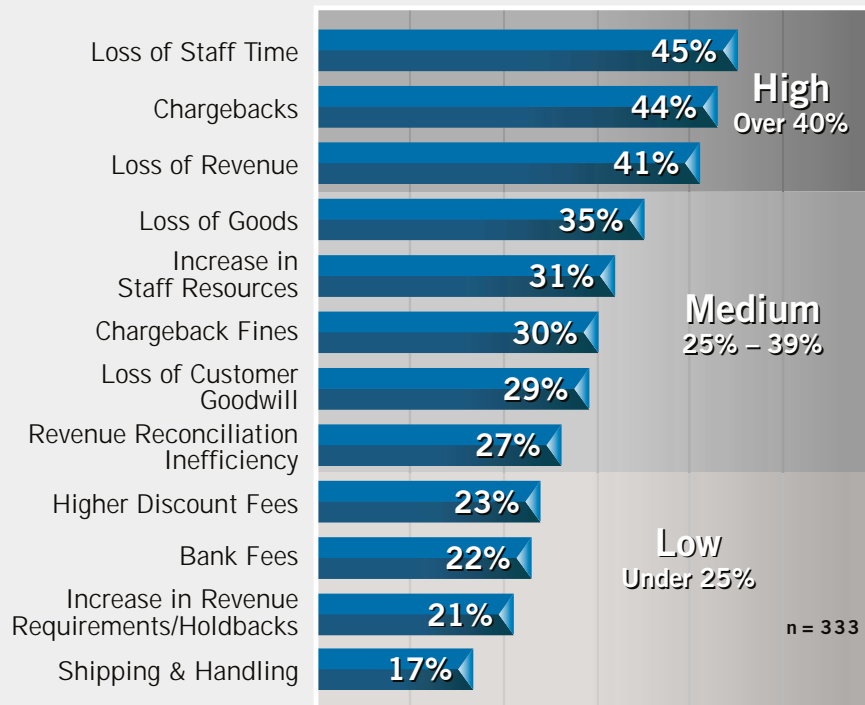


1. Ratio of rejected orders to fraudulent orders is over 3:1
 2. Ratio of rejected International orders 4X U.S. & Canada
 3. Ratio of International fraud 4X domestic fraud
- * Base: Those accepting orders outside USA/Canada.

Negative Impact on Staff Time and Bottom Line

It is important to recognize that total true online credit card fraud costs include more than direct fraud losses and possible revenue losses. Most of these costs and negative impacts are indicated in Chart 5 (below). In addition to the direct losses from online fraud and the indirect cost of rejecting some valid orders, there are significant costs associated with managing the fraud control process. In 2003 as in 2002, merchants reported that the number-one impact of managing online fraud is the loss of staff time, with 45% rating this as a top concern with a substantial negative impact (see Chart 5, below). Indeed, 31% of merchants indicated that the increase in staff resources required to manage fraud has a substantial negative impact on their business. Loss of revenues/goods and chargeback/chargeback fines round out the top six mentions of the substantial negative impacts of online fraud on their business.

Negative Impact of Online Fraud



Loss of staff time, chargebacks, and revenue losses are biggest impacts of online fraud

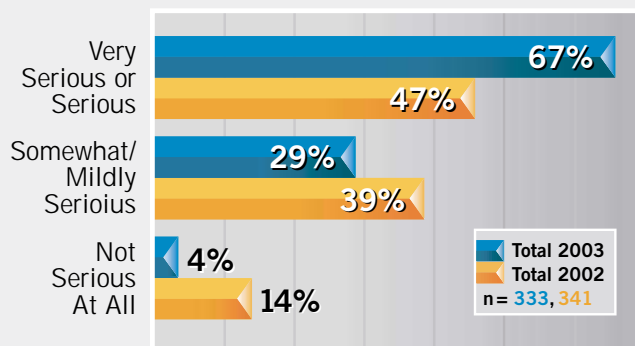
More Merchants Report Online Fraud is a Serious Business Issue

Online credit card fraud remains a significant and serious problem for merchants. While merchants are managing to reduce direct fraud-loss rates, total dollar losses are still high in 2003 due to the continued high growth of online sales. The number of merchants citing online credit card fraud as a "serious" or "very serious" issue for their business increased significantly (see Chart 6, below) to almost two thirds of merchants, despite the drop in the overall average revenue-loss rate, to 1.7%. Perhaps the new rules imposed by card associations to require further reductions in the direct fraud-loss rate are one reason for this increase. It also appears that the costs of managing online credit card fraud are increasing for most merchants. As online sales growth forecasts continue to show growth in excess of 20% over the next few years, it is understandable that most merchants are concerned about managing the online fraud problem cost-effectively, when faced with higher order volumes.

6

% Reporting Fraud as a Serious Business Issue

How serious is the issue of online credit card fraud to your business?



There has been a significant increase in the number of merchants reporting online fraud as a serious issue for their business

III. Common Practices for Managing Online Fraud in 2003

Fraud-Prevention Efforts Increase

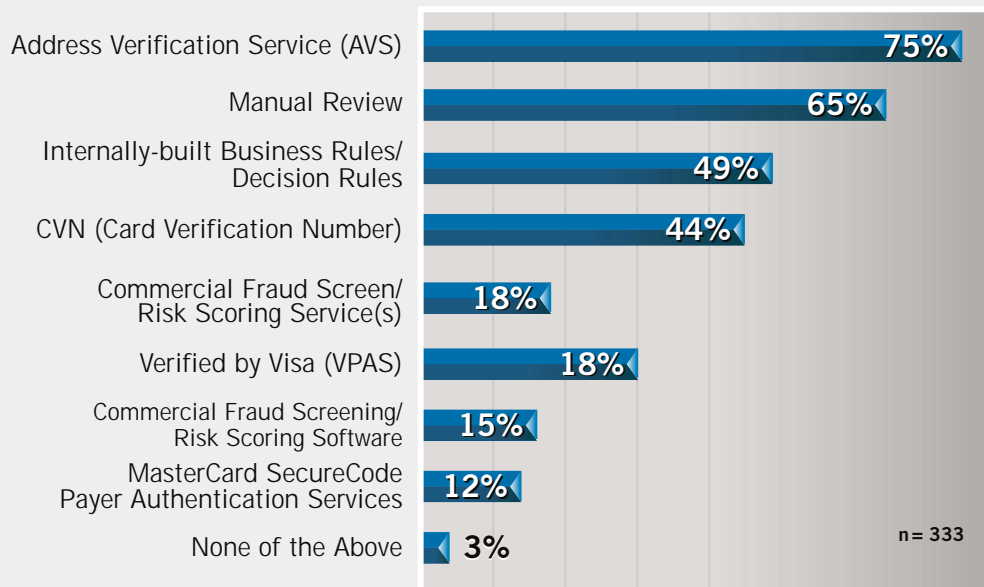
Sixty-nine percent of merchants indicated that they are taking more precautions in 2003 to prevent online fraud, an increase from sixty-five percent in the 2002 survey. Efforts to improve fraud control appear to be something most merchants pursue every year. The survey data shows that as merchants continue to invest in ways to manage and prevent online fraud, they employ a variety of online credit card fraud detection and prevention methods. The most popular methods of deterring online fraud are shown in Chart 7.

More merchants are using the basic fraud protection techniques of manual review, the address verification service, and requesting the shopper to enter the card verification number (CVN) printed on the back of most credit cards.

The most-popular fraud-prevention tool is to request—through the credit card authorization system—cardholder address verification service (known as AVS) from the cardholder's card-issuing bank. 75% of the merchants surveyed indicated that they use AVS as a method of fraud detection. AVS is a relatively simple process, but it is subject to a significant rate of "false positives" which may lead to rejecting valid orders². AVS checks only the numeric data in a street address and postal code. 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 card's issuing bank's records, so the address would be flagged as invalid. As a result of AVS limitations, merchants need to employ additional methods of identifying and managing suspicious orders.

7

Fraud Management Methods

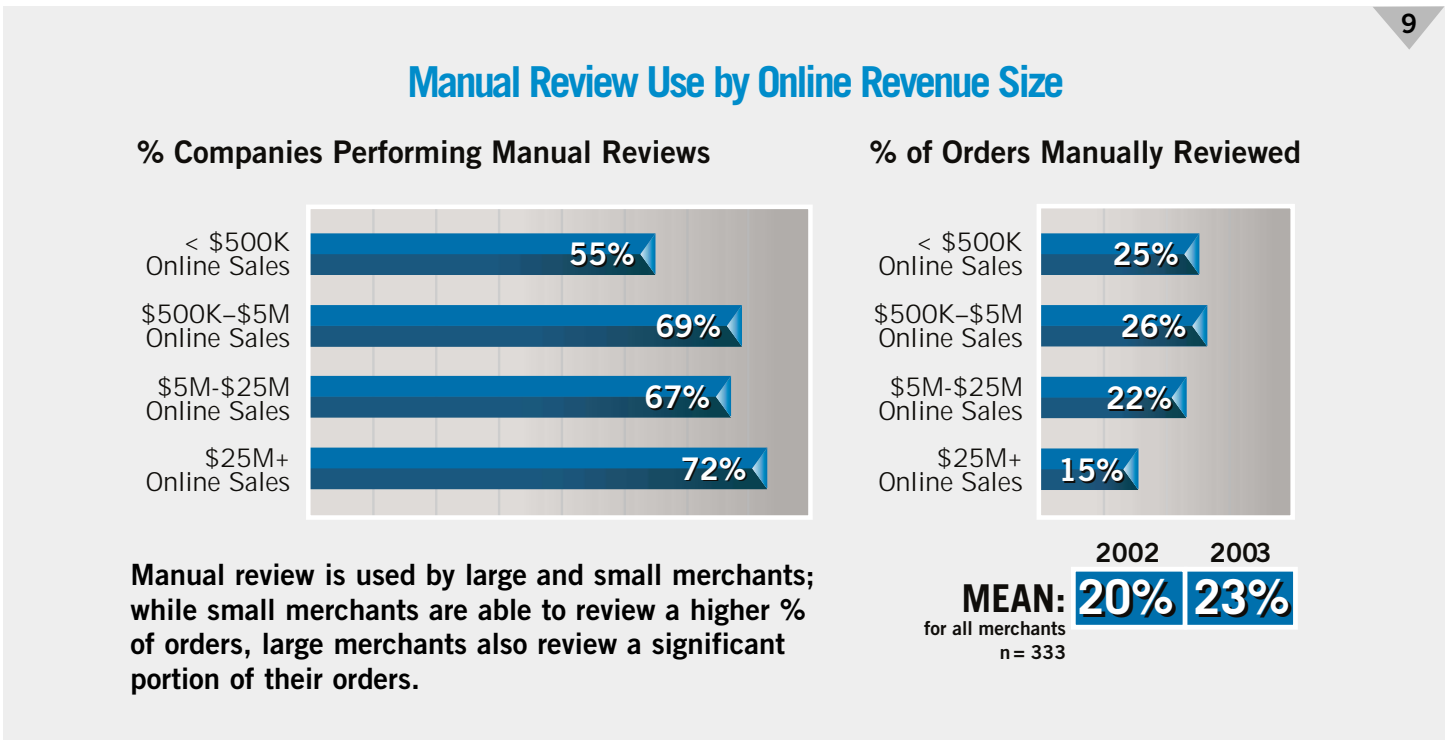
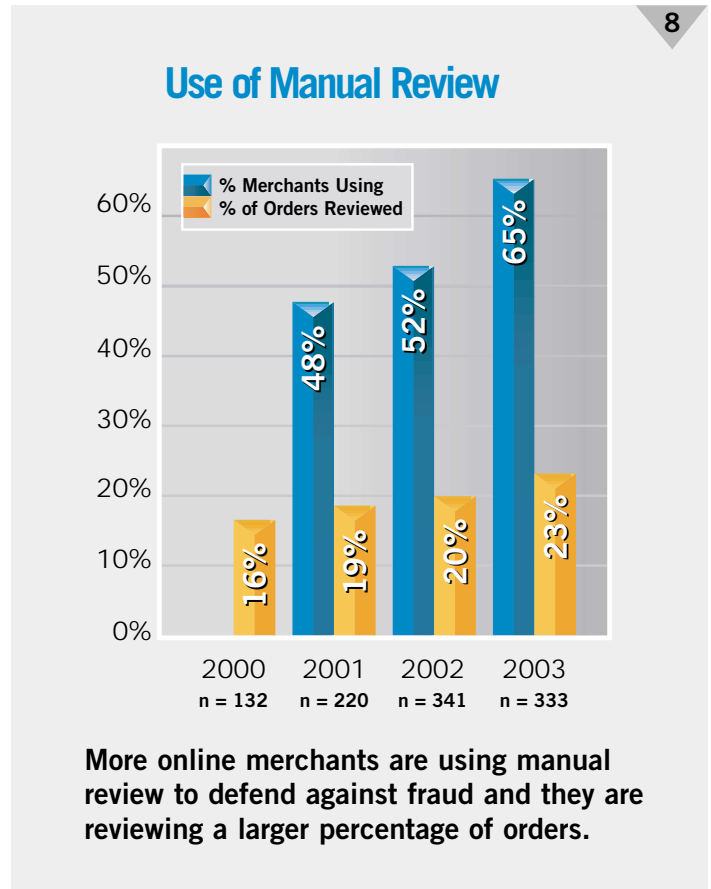


Nearly 2/3rds of merchants now use manual order review to manage fraud – this is now the second most popular method, moving up from third place last year.

Manual Intervention Efforts Continue to Increase

The second-most-popular method of fraud prevention in 2003 is manual order review. This survey indicates a significant increase in the percentage of merchants employing manual review to control online credit card fraud. Manual review is now used by 65%, or almost two-thirds, of merchants, a 13-point increase from 2002, and up from less than 50% in 2001. In addition to more merchants using manual review, the average proportion of orders reviewed is now approaching one out of every four. Over the past four years, we have seen a steady increase in manual review, from 16% in 2000 (approximately one in six orders), to 23% in this survey (see Chart 8).

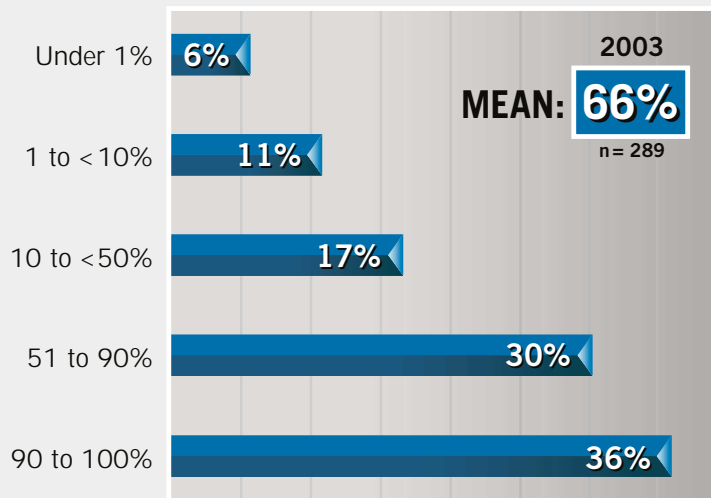
While manual review may be viable for smaller merchants with low order volumes, it is not normally a cost-effective or scalable solution for larger merchants with high order volumes or seasonal order peaks. In fact, the survey data shows that while the largest merchants (over \$10 million in annual online sales, representing 28% of the merchants responding to the survey) use manual review methods more often than the overall sample average, they review a smaller percentage of their orders. Almost three-quarters of large merchants report using manual review as a tool to detect and prevent online fraud (as shown in Chart 9), although smaller merchants review more orders on average (25% of orders received) than large merchants (15% of orders).



While the percentage of online orders being reviewed manually is only up three points in 2003, the volume of online sales is up (according to most sources³) by 25 - 30%, or more. As a result, merchants have to manually investigate many more orders in 2003 than they did in 2002. Most online sales forecasts continue to project a 25 - 35% annual growth rate over the next few years, indicating that merchants who manually review a significant portion of orders will need to either divert more staff time to the order review process, increase staffing levels, allow more time to process orders and ship goods, or take the risk of reducing the rate at which they review suspicious orders.

Interestingly enough, on average, merchants surveyed indicated that they ultimately accept two-thirds of the orders they decide to manually review (see Chart 10). Many merchants are accepting more than 90%. Clearly a significant amount of human effort and cost is going into identifying the orders to reject. It also indicates that, based on the averages, the actual order rejection rate could be higher than the 3.4% directly reported by merchants in the survey. Since 34% of orders are rejected out of a total of 23% of all orders reviewed, this would imply an order-rejection rate of 7.8% —or approximately double the direct rejection rate reported by merchants.

% of Manually Reviewed Orders Ultimately Accepted



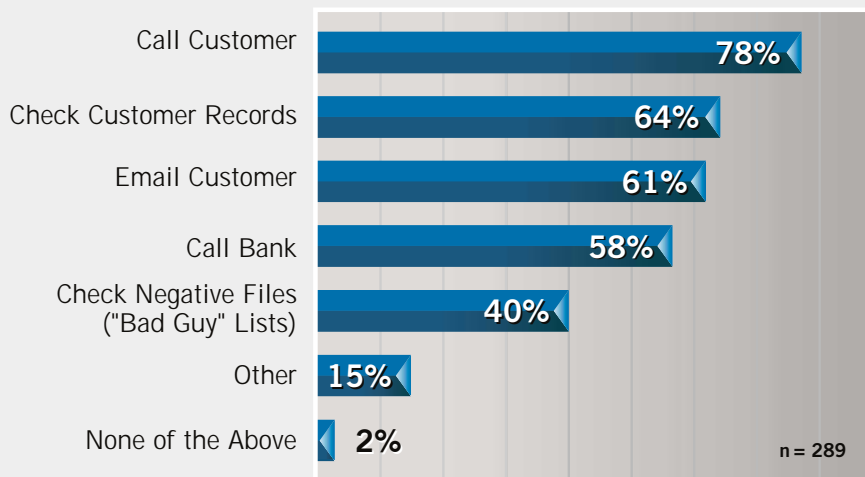
After manual review most orders are accepted by merchants.

The problem of relying on manual intervention to prevent fraud goes beyond the lack of scalability and cost, as most manual-review techniques involve contacting the consumer to validate online order information or to collect additional information. As shown in Chart 11 (below); two of the top three methods employed during the manual-review process require that the merchant re-engage the customer in the order process. This additional exchange with the customer could result in delayed shipments and higher levels of customer dissatisfaction.

There is no single "tried-and-true" solution to the problem of managing and reducing the costs of online fraud. Just as fraudsters use a variety of ever-changing techniques to commit online credit card fraud, merchants must use a variety of methods to manage the problem in a cost-effective way. Merchants face several challenges in managing online fraud, including keeping fraud tools and strategies tuned and up-to-date on a regular basis, as well as intelligently applying the variety of tools required to reduce fraud, increase operational efficiency, maximize sales, and minimize the negative impacts of fraud protection measures on customers. Survey results continue to indicate that merchants are struggling to meet all of these objectives and increase their Return on Investment (ROI) for fraud-management efforts. Merchants are seeing relatively minor reductions in total online fraud dollar losses while experiencing significant increases in staff time/costs. However some merchants have achieved lower fraud rates and significant ROI for fraud management efforts through the careful application of best practices to the entire order flow process (for more information see references in the Resources section later in this report).

11

Manual Review Techniques



Two of the top three manual techniques used require merchants to re-engage the customer to process the order

IV. Plans for Managing Online Fraud in 2004

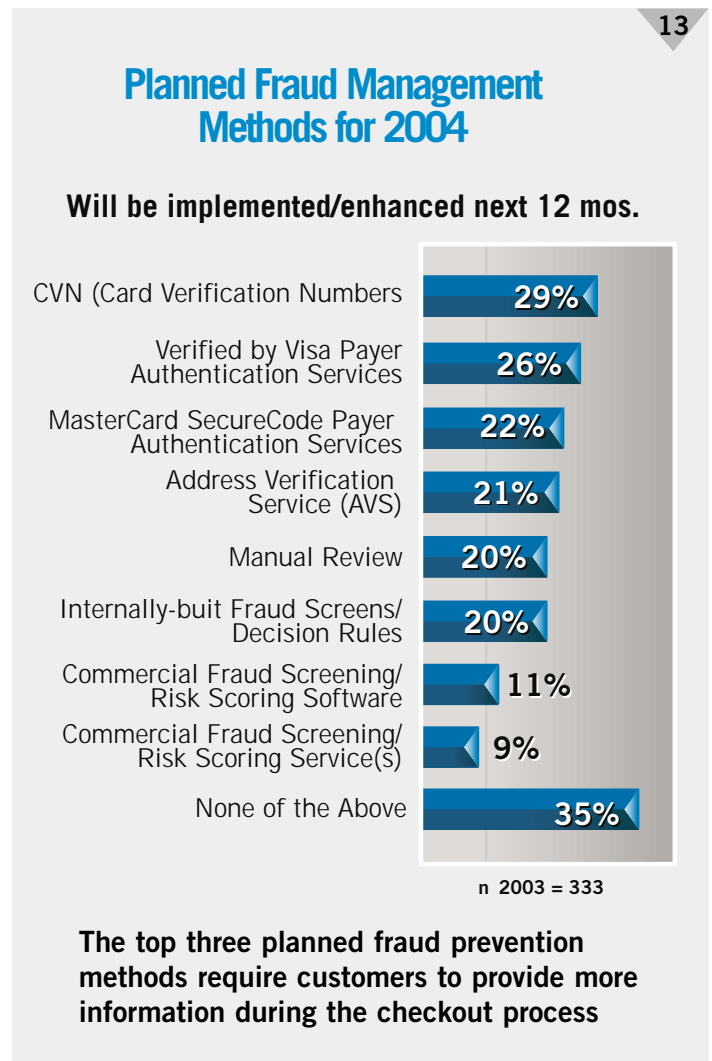
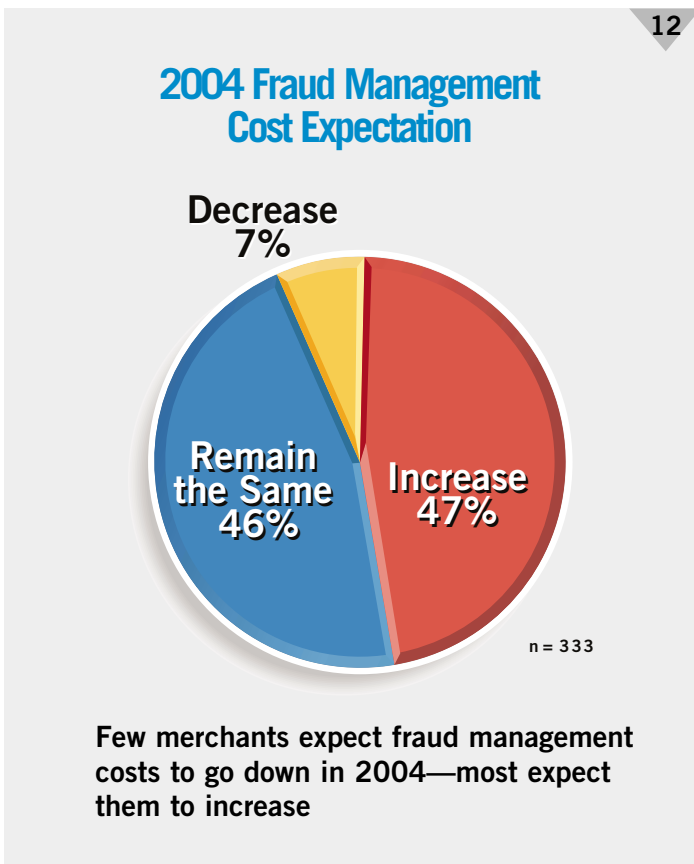
Most Merchants Expect Fraud-Control Costs to Increase

Increased use of manual review to control online credit card fraud, along with the high growth of online sales, has resulted in a cost-control problem for many merchants. Only 7% of merchants surveyed expect their fraud control costs to decline in 2004; 47% of merchants expect fraud control costs to increase in that year (see Chart 12).

It is clear that many merchants need to invest in tools and processes to increase the productivity and effectiveness of employees responsible for managing online fraud. For most merchants, it is unlikely that human intervention can be eliminated completely from the order review and acceptance process. The focus must be on how to maximize the productivity and effectiveness of the manual review process so that as online order volume grows, additions to staff to control online credit card fraud can be minimized.

Consumers Will be Asked to Provide More Information

Two-thirds of merchants plan to adopt one or more new methods to prevent and manage online fraud in 2004. As we saw in last year's survey, and as Chart 13 (below) indicates, the most popular methods merchants plan to add or enhance over the next year require consumers to provide more information during the checkout process. Asking consumers to provide the CVN number on the back of most credit cards or to enter a password to authorize a purchase are the most popular techniques merchants plan to implement.



Visa and MasterCard have introduced password-based programs to allow registered cardholders to verify their purchases, a process known as payer authentication. Merchants who adopt these new online checkout procedures may receive increased protection from chargebacks and may receive lower discount fees. This survey shows an increase in the number of merchants implementing these systems and an increase in awareness about these relatively new approaches to managing online fraud (see Chart 14). However, concerns still exist about the impact these new password-based systems have on the checkout process (e.g. will consumers forget their passwords and not be able to complete the checkout process, etc.), and about the level of cardholder adoption.

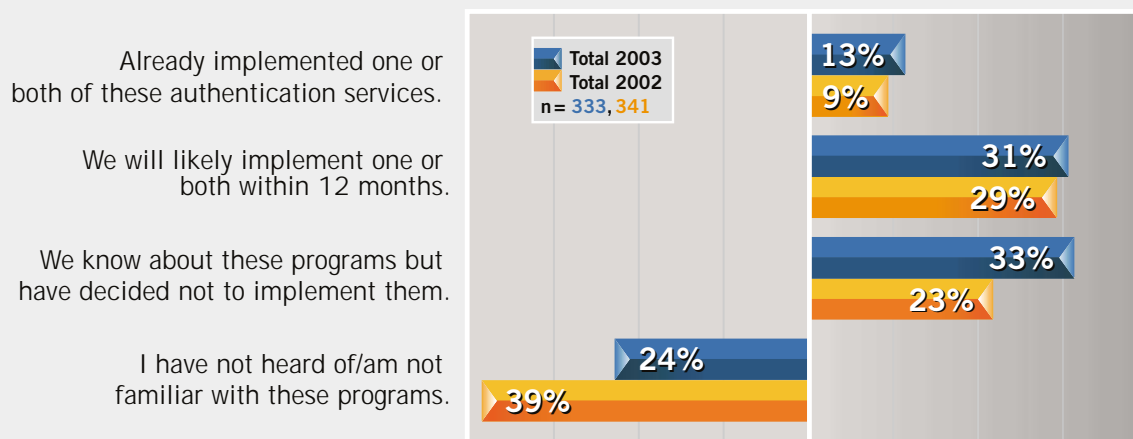
Implementation of payer authentication systems can reduce a merchant's liability for fraudulent credit card charges. If merchants have a high direct fraud-loss rate, however, they will not be eligible for chargeback protection even if they have implemented a payer authentication system. Over the next few years, these systems may help reduce the incidence of online credit card fraud if most consumers register their cards and accept the new checkout procedures. At this time it remains uncertain how quickly consumers will adopt these new methods of online shopping. It is unlikely that consumer adoption will reach 100% in the next few years, so merchants will still need to have procedures in place to handle customers who have not adopted the new systems or who use cards other than Visa and MasterCard to make purchases.

Conclusion

Successful and cost-effective management of online fraud control in 2004 will continue to depend upon the intelligent planning and deployment of processes and technology to manage the order review and acceptance process efficiently and effectively. Businesses that manage to increase employee productivity and the efficiency of the order review process will likely succeed in seeing online revenue growth translate fully into bottom-line profit growth. Those who are unable to increase efficiency in the order review and acceptance process will likely continue to be squeezed by rising costs and lost revenues associated with online credit card fraud.

14

Adoption of Visa & MasterCard Payer Authentication



Awareness of card associations' new payer authentication Systems has increased, but actual adoption has been slow.

Resources

Find these additional resources—as well as product data sheets—located on the CyberSource web site at www.cybersource.com/resourcecenter/.

- [Internet Retailer Article: PC Mall trims fraudulent transactions to less than 1% with CyberSource tool](#)
- [Internet Retailer Article: Finish Line Tackles Online Fraud](#)
- [Case Study: CompUSA Jumps on Fraud with CyberSource](#)
- [New Payment Rules Change Online Retail 2003 \(Guide to Verified by Visa and MasterCard SecureCode Payer Authentication programs\)](#)
- [CyberSource Payer Authentication Product Brief](#)
- [CyberSource Advanced Fraud Screen](#)

CyberSource Risk Management Solutions

Efficiently managing online fraud involves integrating multiple tools and technologies to maximize operational efficiency and sales conversion, while minimizing fraud risk. CyberSource customers achieved significantly better results than other merchants in this survey due to the effective deployment of CyberSource's suite of modular, scalable solutions (For additional performance data please contact a CyberSource representative). These solutions can be quickly and easily implemented as a single component or as fully-integrated systems and can be managed in-house, outsourced or as a blend of both options.

CyberSource Risk Management Solution – Complete Enterprise Platform

Automated decision platform and expansion modules make it easy to create and manage order processing rules and risk indicators. Using product, industry, and channel variables in real-time via a single business interface, Risk Manager seamlessly integrates to external information services as well as to internal lists from company databases. Risk Manager improves the efficiency and effectiveness of staff managing the order acceptance process.

CyberSource Advanced Fraud Screen Enhanced by Visa

Using CyberSource technologies, highly accurate order evaluation scores are typically calculated in less than two seconds. This service is further enhanced by Visa's patent-pending Virtual Intelligence Risk Technology (VIRT). VIRT improves fraud detection accuracy by providing continuous model updates based on global fraud trends and online/offline payment card usage patterns. Advanced Fraud Screening helps merchants separate their order mix into Approve, Review and Reject work flows.

CyberSource Verification and Compliance

CyberSource offers Delivery Address Verification (DAV) services to verify the validity of addresses worldwide and comply with USPS postal 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 to comply with U.S. Government Bureau of Export Administration (BXA) procedures involving denied party and denied country checking, as well as internal company policies regarding countries to which shipment is permitted.

CyberSource Payer Authentication – Online Cardholder Validation

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. Deploy now to gain the benefits of increased cardholder confidence, enhanced chargeback protection, and optimum card association interchange rates.

CyberSource Payment

CyberSource offers complete payment processing services including credit cards, electronic checks, gift certificates and tax calculations.

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/IVR, and POS environments and manage transaction risk associated with card-not-present transactions. CyberSource Professional Services designs, integrates, and optimizes enterprise-wide commerce transaction systems. Over 3,000 businesses use CyberSource solutions, including over half of the Dow Jones Industrial companies. 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.

For More Information

- Call 1-888-330-2300
- Email info@cybersource.com
- Visit www.cybersource.com

1 Internet Retailer Sept 4th, 2003

2 CyberSource recently 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 on AVS "no match" they would incorrectly reject 25% of the good orders and fail to detect 61% of the fraudulent orders.

3 U.S. Census Bureau, United States Department of Commerce, Third Quarter Retail E-Commerce Survey

United States

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 Europe
400 Thames Valley Park Drive
Thames Valley Park
Reading RG6 1PT
United Kingdom
T: +44 (0) 1189.653.819
F: +44 (0) 870.460.1931
Email: 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