

ONLINE FRAUD REPORT

Online Credit Card Fraud Trends and Merchants' Response

2002 Results

Sponsored by CyberSource Corporation

Conducted by Mindwave Research

CyberSource®

Table of Contents

Executive Summary	4
Key Findings & Analysis	4
Conclusions	5
Methodology	5
Business Impact of Online Fraud in 2002	6
Finding: Online Fraud Rate Unchanged	6
Finding: Negative Impact On Staff Time And Bottom Line	8
Managing Online Fraud in 2002	9
Finding: Fraud Prevention Efforts Increase	9
Finding: More Manual Intervention	10
Managing Online Fraud in 2003	14
Finding: Consumers Will be Asked to Provide More Information	14
CyberSource Fraud Management Solutions	16
CyberSource Payer Authentication – Online Chargeback Protection	16
CyberSource Advanced Fraud Screen Enhanced by Visa – Highly Accurate Scoring	16
CyberSource Risk Management Solution – Complete Enterprise Platform	16
Additional CyberSource Products and Services – Payment, Verification and Compliance	16
About CyberSource	16

Figures

Chart 1. % of Revenue Lost to Fraud	6
Chart 2. % of Fraudulent Transactions	6
Chart 3. Online vs. Offline Fraud	7
Chart 4. Anticipated Holiday Season Fraud	7
Chart 5. Negative Impacts of Online Fraud	8
Chart 6. Fraud Precautions	9
Chart 7. Fraud Management Methods	10
Chart 8. % of Merchants Using Manual Order Review	11
Chart 9. % of Orders Manually Reviewed	11
Chart 10. % of Orders Needing Manual Review	12
Chart 11. Manual Review Techniques	13
Chart 12. Implementation Plans for 2003	14
Chart 13. Fraud Management Methods for 2003	14
Chart 14. New Visa and MasterCard Authentication Programs	15

Executive Summary

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

- Online fraud's impact on business operations
- Merchant efforts to manage fraud
- Plans to combat online fraud in the future (including new payer authentication systems from Visa and MasterCard)

Key Findings & Analysis

Fraud Rates

Online fraud rates in 2002 did not significantly change from 2001. They remained at an average of 3% of revenues for surveyed merchants. But because online sales volume grew 30+% in 2002, a constant fraud rate means that actual dollars lost to fraud increased.

Use of Anti-Fraud Tools

More merchants used more tools to manage and protect themselves from online fraud in 2002. Despite such utilization, their fraud losses did not decrease. This suggests that merely increasing the number of anti-fraud tools is not enough. To create an effective fraud management system, merchants must also integrate these tools into an overall order review and acceptance process. The tools and techniques must be updated and tuned regularly to remain effective, as perpetrators develop new ways to commit online fraud.

Of special note: Some large online merchants managed to reduce their fraud rates significantly below 3% of revenue while maximizing valid order acceptance.¹ By applying best practices, merchants can achieve a more effective fraud management system.

Staff Cost of Manual Review

Employee intervention to detect and prevent fraud in 2002 increased significantly at merchants of every size. Specifically, manual review was used by more merchants. It was the second most popular method for managing online fraud after the use of Address Verification Service (AVS) during the credit card authorization process.

On average, merchants manually reviewed 20% of online orders in 2002; up from 19% reported in 2001. Surprisingly, manual review was not limited to smaller merchants who process fewer orders. It was also used by many of the largest online retailers. Because online sales increased approximately 30% in 2002, it is likely that most online merchants incurred additional staff costs – increased hiring and overtime – to review orders manually.

Consumer Cost of Manual Review

Contacting customers by phone or email were two of the top three manual review techniques that surveyed merchants used to verify orders in 2002. In fact, most manual review processes 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. It is, therefore, likely that increased reliance on manual review will result in lost sales or fewer repeat purchases.

¹ CompUSA case study, available online – www.cybersource.com/cgi-bin/resource_center/resources.cgi.

Payer Authentication Systems

A significant number of the merchants surveyed plan to adopt new Visa and MasterCard cardholder authentication systems in 2003. These systems ask online shoppers to provide a password during the checkout process. This enables merchants to authenticate credit card orders with the cardholder's issuing bank. Implementing these systems will reduce the merchant's liability for fraudulent charges.

In addition, more merchants plan to ask consumers to locate and provide the card verification numbers on their credit cards during the checkout process in 2003 (these are known as CVV for Visa, CVC for MasterCard and CID for American Express and Discover).

Merchants will need to closely monitor the impact of asking customers to provide additional payer authentication information if they implement these systems in 2003. They will need to carefully architect the implementation and integration of these new tools in order to minimize the disruption of the online shopping experience for consumers.

Conclusions

Despite increased efforts by merchants to manage online fraud in 2002, total fraud losses continued to escalate. The survey shows that current fraud management practices place a significant emphasis on manual intervention. However, relying too heavily on manual intervention leads to increasing costs as online sales continue to grow.

Current approaches to managing fraud are likely to result in increased costs as online order volumes grow. Recent data from the U.S. Department of Commerce indicates that online sales are growing in excess of 30% annually². Therefore, merchants need (a) improved practices in applying fraud management tools and processes, (b) more automated solutions to reduce fraud losses and associated fraud management costs and (c) to deploy multiple fraud-prevention tools and strategies to battle the increasing number of fraud methods being employed.

The survey also shows that future plans to manage fraud require more information and involvement from online shoppers. Placing more of the authentication burden on consumers may negatively impact the online shopping experience. This needs to be carefully managed to avoid reducing repeat purchases or increasing shopping cart abandonment rates.

Methodology

Merchants invited to participate reflected a blend of small-, medium- and large-sized businesses. They range from companies in their first year of online transactions to the largest e-retailers in the world. Over 55% of the merchants surveyed had both an online and offline (brick and mortar) business presence.

The survey was conducted via an online questionnaire at the Mindwave Research website. Three hundred forty-one merchants completed the survey between October 2nd and October 9th, 2002. All participants were either responsible for or influenced decisions regarding risk management in their companies.

² U.S. Census Bureau, United States Department of Commerce, Third Quarter Retail E-commerce Survey (2002).
Retrieved from: <http://www.census.gov/mrts/www/mrts.html>

SUMMARY OF PARTICIPANTS' PROFILES

Annual Online Revenue

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

Duration of Online Selling

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

Risk Management Responsibility

Ultimately Responsible	32%
Influence Decision	68%

Sales Channels

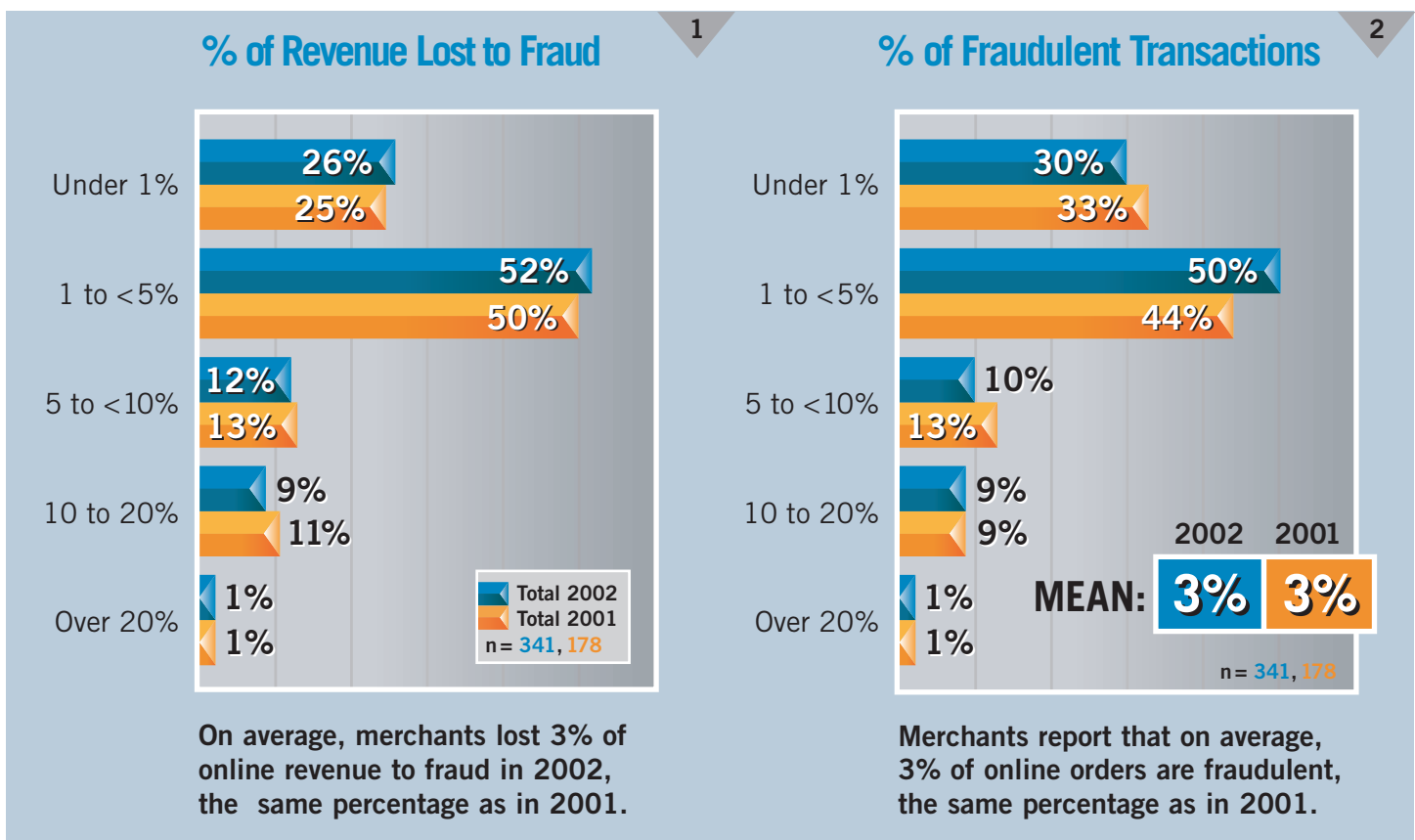
Online Store only	45%
Both Online and Physical Stores	55%

Business Impact of Online Fraud in 2002

Finding: Online Fraud Rate Unchanged

A key finding of the fourth annual online fraud survey is that merchants report no significant change in the rate of revenue loss due to online fraud. As Chart 1 (below left) shows, merchants are losing on average, 3% of online revenues to fraud, the same level reported in 2001. The data also indicates that 22% of merchants report a serious fraud problem, with 5% or more of online revenues lost to fraudulent credit card activity annually.

The incidence of fraudulent orders reported by merchants is also unchanged from 2001 as shown in Chart 2 (below right). In 2002, online merchants report that on average, 3% of online orders were fraudulent. Twenty percent of merchants surveyed report higher rates (5% or more of online orders).

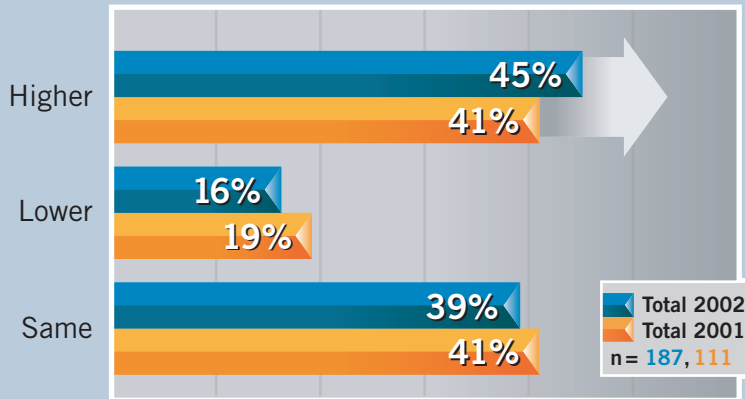


Most U.S. online sales estimates indicate that annual online revenues are growing by 30% or more. Since the rate of fraudulent orders and the percent of revenue lost to fraud remains unchanged, the total dollar fraud losses by U.S. online merchants have also increased by 30% or more, staying in line with overall sales growth.

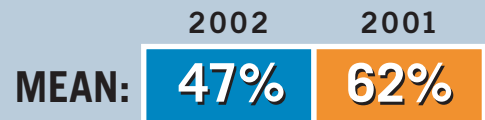
Online fraud is also a significant problem for merchants selling through online and traditional sales channels (such as retail stores or call centers). Chart 3 (following page) indicates that, on average, "brick and mortar" retailers find that online fraud losses are as high as, or higher than, sales through offline channels. Forty-five percent of the merchants indicate that online fraud losses are higher than offline losses, and 39% report they are equal. Merchants reporting higher fraud losses indicate that online sales channel losses average nearly 50% higher than offline channels, even though offline sales tend to be considerably larger.

Online vs. Offline Fraud

How Does Online Fraud Compare To Offline?



How Much Higher?



Base: Those whose online credit card fraud was higher than offline

n = 84,45

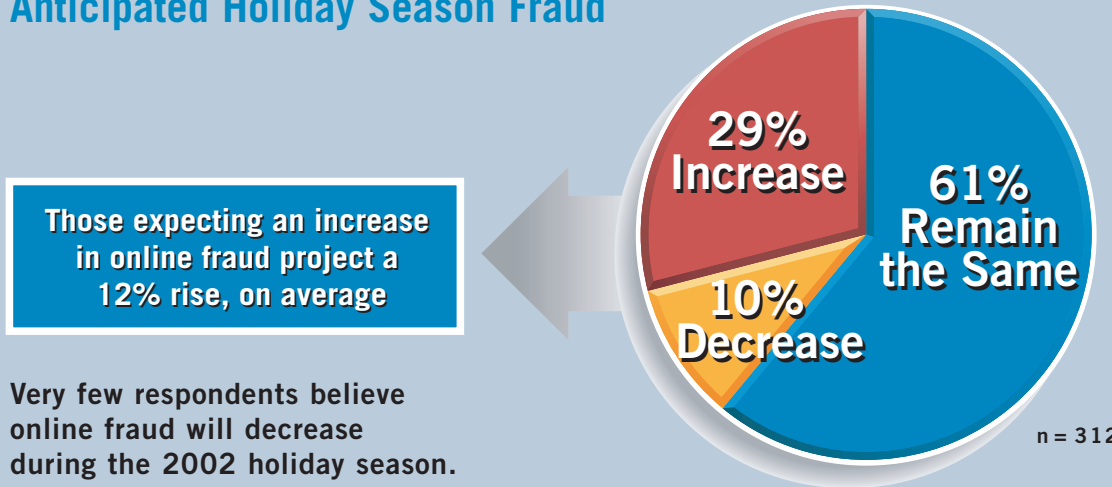
Base: Those who sell both online (web) and offline (storefront/callcenter)

Online fraud typically higher than offline fraud in 2002

This survey was conducted just prior to the start of the 2002 peak holiday sales season. Merchants were asked about their expectations of online fraud levels during the peak online sales season.

Chart 4 (below) indicates that 29% of merchants expect online fraud levels to increase during the peak selling season and only 10% expect them to decrease. The merchants who expect an increase in fraud levels during the peak holiday sales period estimate an average increase of 12%.

Anticipated Holiday Season Fraud



Those expecting an increase in online fraud project a 12% rise, on average

Very few respondents believe online fraud will decrease during the 2002 holiday season.

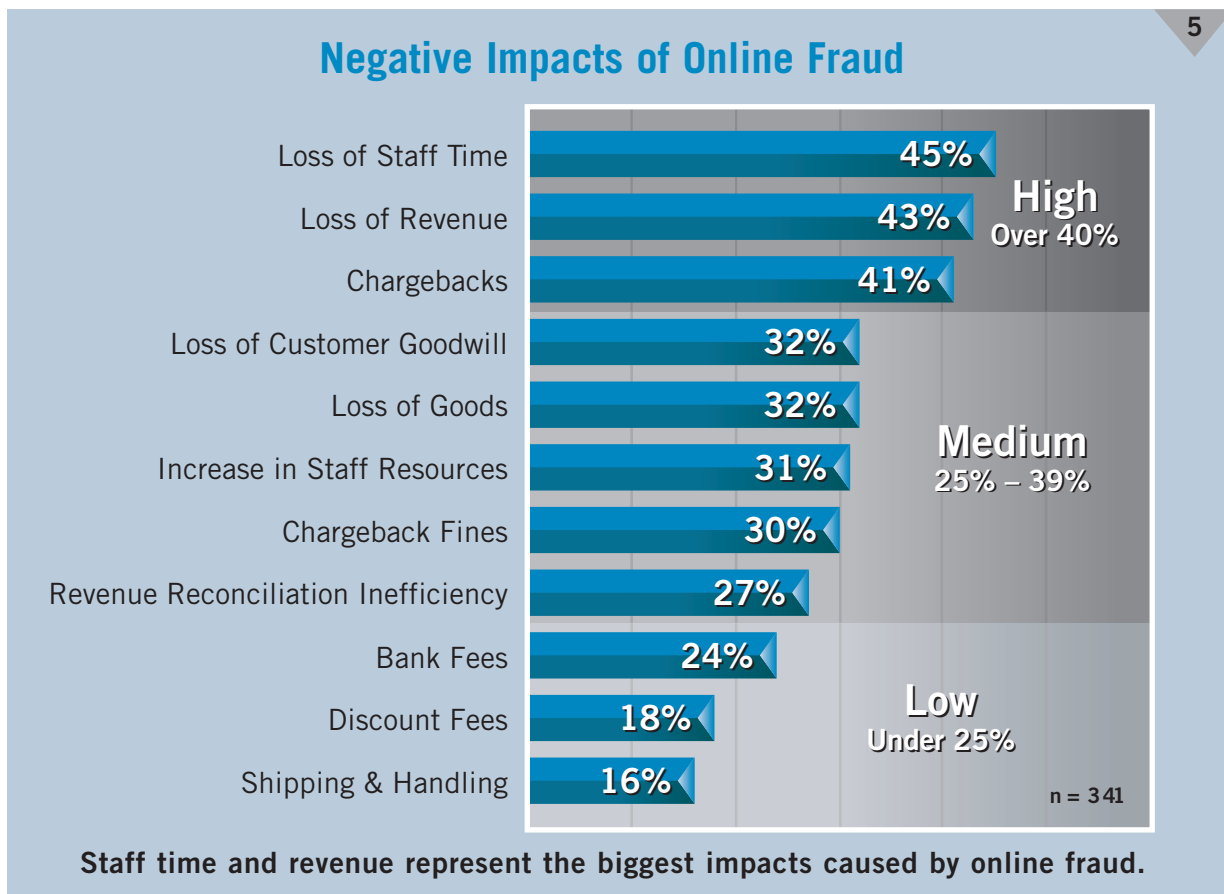
Finding: Negative Impact On Staff Time And Bottom Line

It is important to recognize that online credit card fraud costs include more than direct revenue losses. Most of these are indicated in Chart 5 (below), including such costs as chargeback fines, bank fees, increased discount rates, reconciliation and auditing costs, etc.

In addition to the direct losses from online fraud, there are significant costs associated with managing the growing number of fraudulent orders. Merchants report that one of the most significant costs of online fraud is the loss of staff time. As shown in Chart 5, merchants' concerns about loss of staff time surpasses the negative impact of direct revenue losses.

Although merchants were not surveyed as to the percentage of suspicious orders they refused, the order rejection rate may often exceed the actual fraudulent order rate. It is possible that many rejected online orders are valid; rejecting them due to their suspicious nature results in lost revenue and is another significant online fraud management cost.

Overall, data from the 2002 survey indicates that online credit card fraud remains a significant and serious problem for online merchants. Total losses to online fraud are on the rise despite increased prevention efforts by merchants. Online merchants appear to be "running harder" just to keep fraud rates from rising.

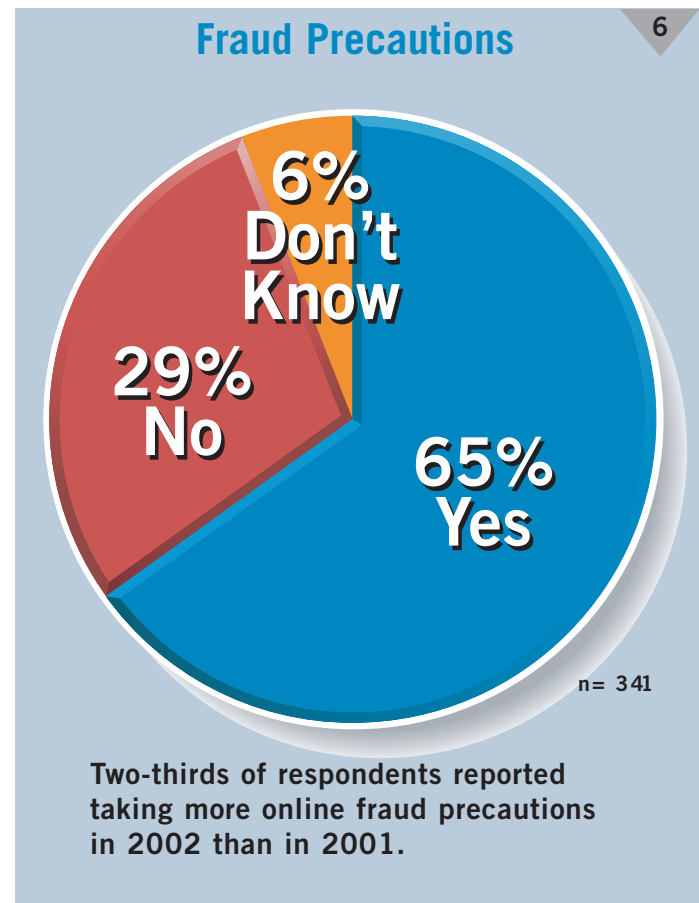


Managing Online Fraud in 2002

Finding: Fraud Prevention Efforts Increase

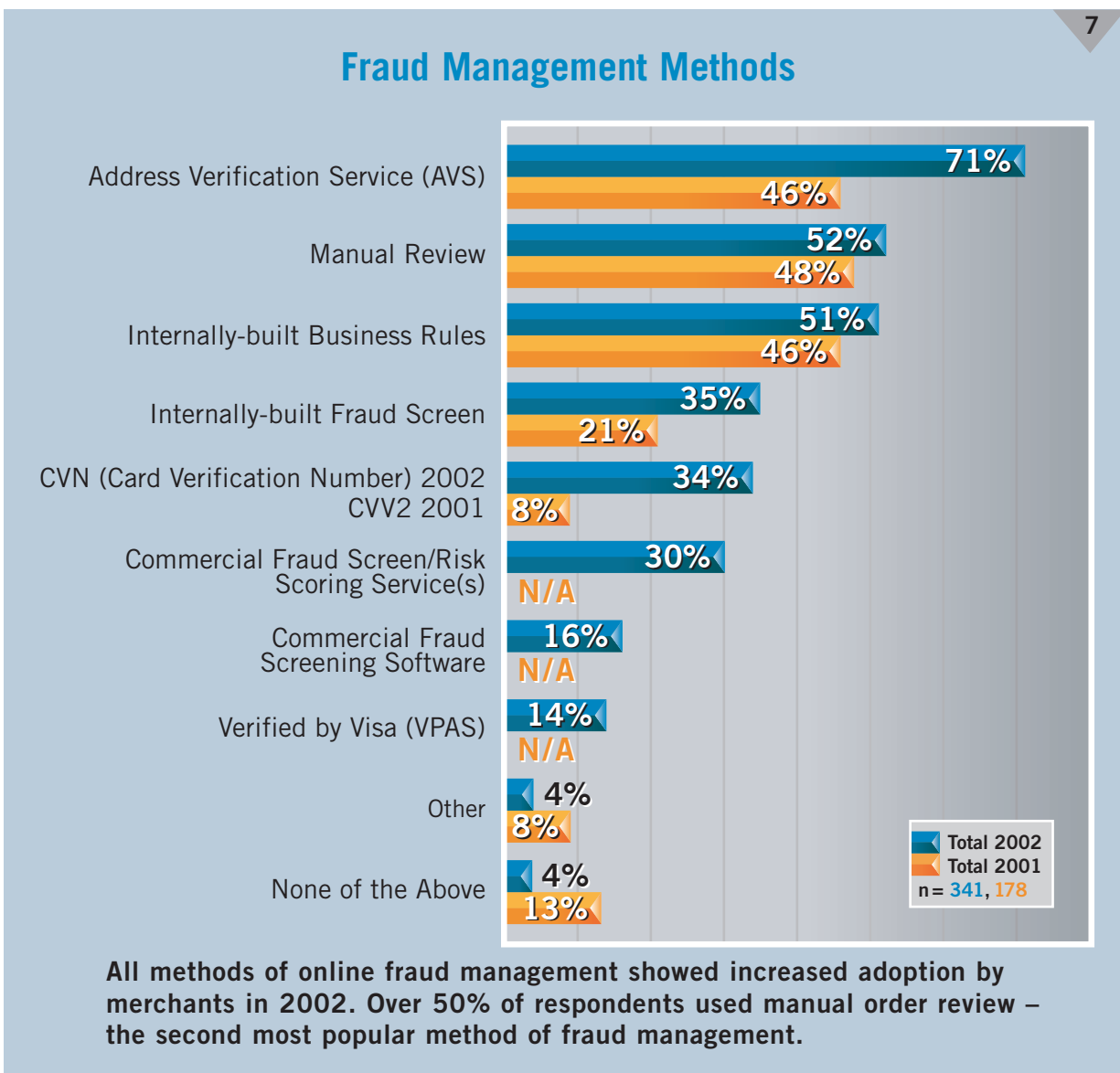
Sixty-five percent of online merchants indicate that they are taking more precautions this year to prevent online fraud as shown in Chart 6. The survey data shows that as merchants continue to invest in ways to manage and prevent online fraud, they employ a variety of online credit card fraud detection and prevention methods. The most popular methods of deterring online fraud are shown in Chart 7 (following page). Each method mentioned in the survey is used by more of the online merchants in 2002 than in 2001.

The most popular fraud-prevention tool is to request, through the credit card authorization system, cardholder address verification (known as AVS) from the cardholder's card issuing bank. Seventy-one percent of the merchants surveyed indicate 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 orders. Since AVS only checks the numeric data in a street address and zip code, an AVS "no match" response is common. 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 card's issuing bank, so the address would be flagged as invalid. There are other common reasons for a false AVS result such as a customer accidentally transposing numbers in a street address or zip code. As a result of AVS limitations, merchants need to employ additional methods of identifying and managing suspicious orders.



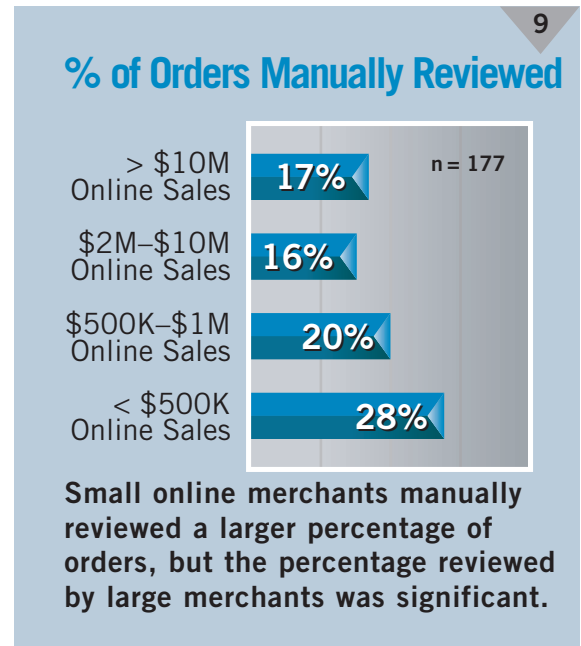
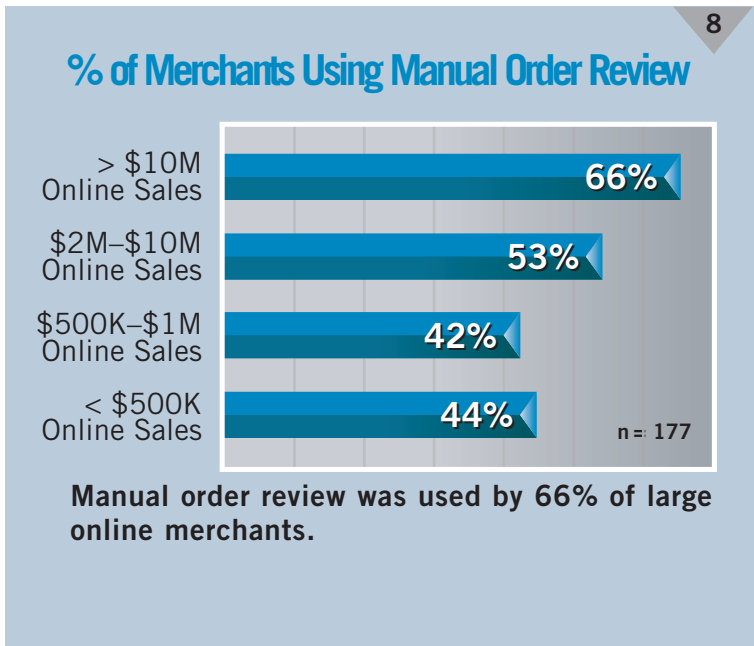
Finding: More Manual Intervention

The second most popular method of fraud prevention is manual order review. More than half of online merchants use this approach, as shown in Chart 7 (below).

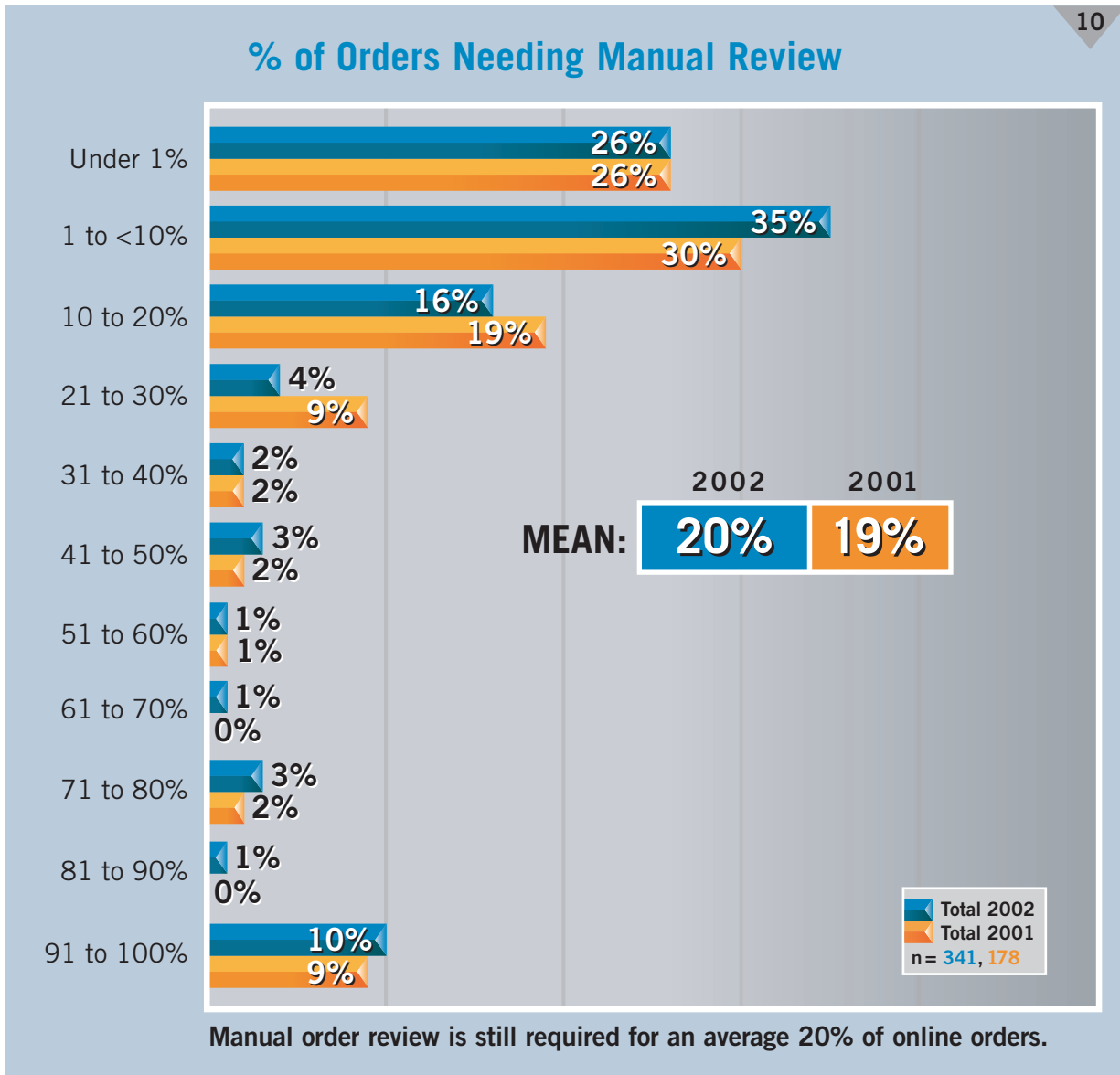


While manual review may be viable for smaller online merchants with low order volumes, it is not normally a cost-effective or scalable solution for larger online merchants with high order volumes or seasonal order peaks.

In fact, the survey data shows that while more of the largest online 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 smaller percentage of their orders. Two-thirds of large online merchants report using manual review as a tool to detect and prevent online fraud as shown in Chart 8 (below left). Small online merchants review more orders on average (28% of orders received) than large online merchants (17% of orders), as shown in Chart 9 (below right).

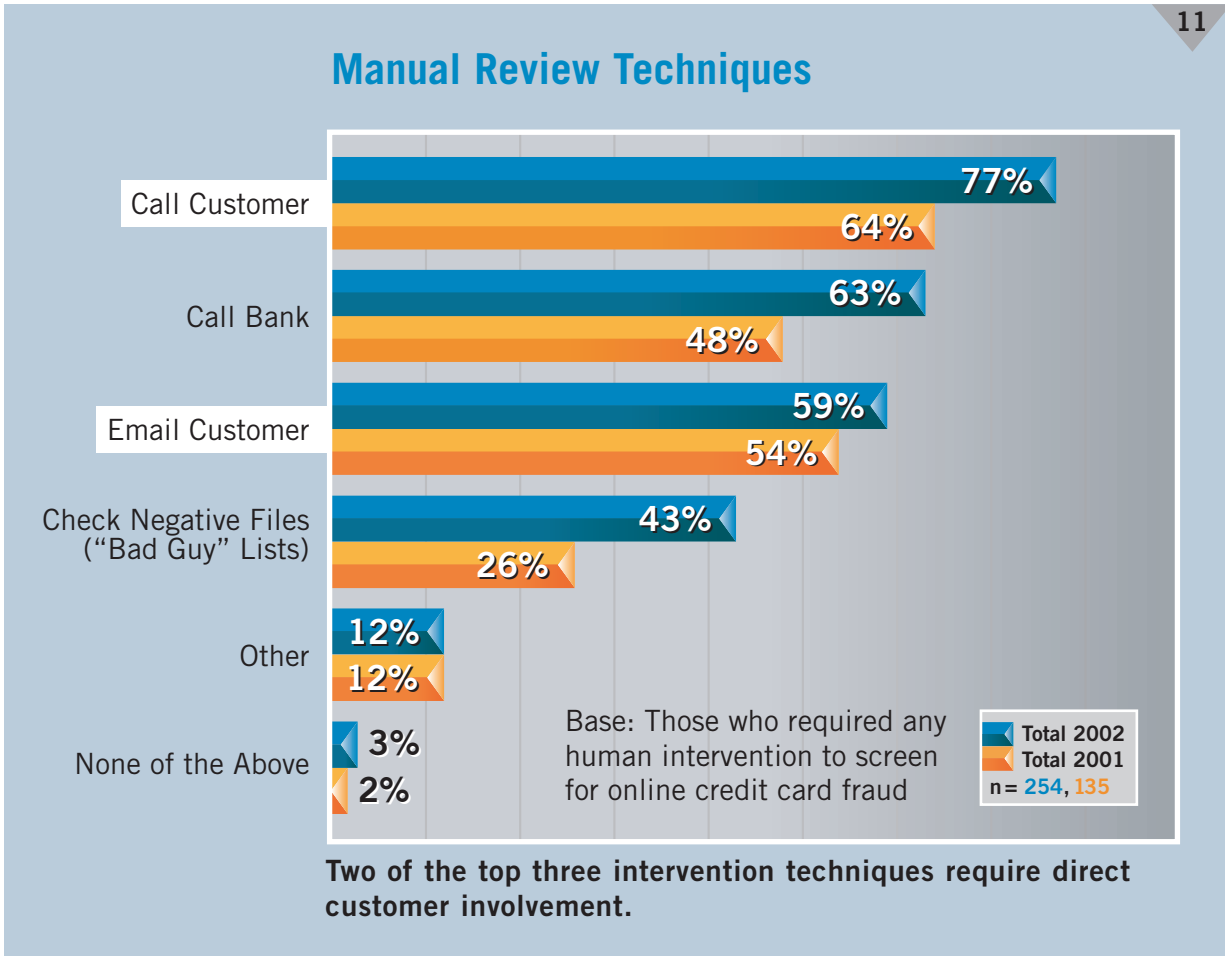


Merchants report that they review on average, one out of every five orders (20%) as indicated in Chart 10 (following page). Twenty-five percent of merchants report reviewing more than 20% of their orders, and 10% of merchants report reviewing 90% or more.



While the percentage of online orders being reviewed manually is only up slightly in 2002, the volume of online sales is up (according to most sources) by 30% or more. As a result, online merchants have to investigate manually many more orders in 2002 than they did in 2001. Most online sales forecasts continue to project a 25 – 35% annual growth rate over the next few years, indicating that online merchants who manually review a significant portion of orders will need to divert more staff time to the order review process, either increasing staffing levels or reducing the rate at which they review suspicious orders.

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 customer dissatisfaction.



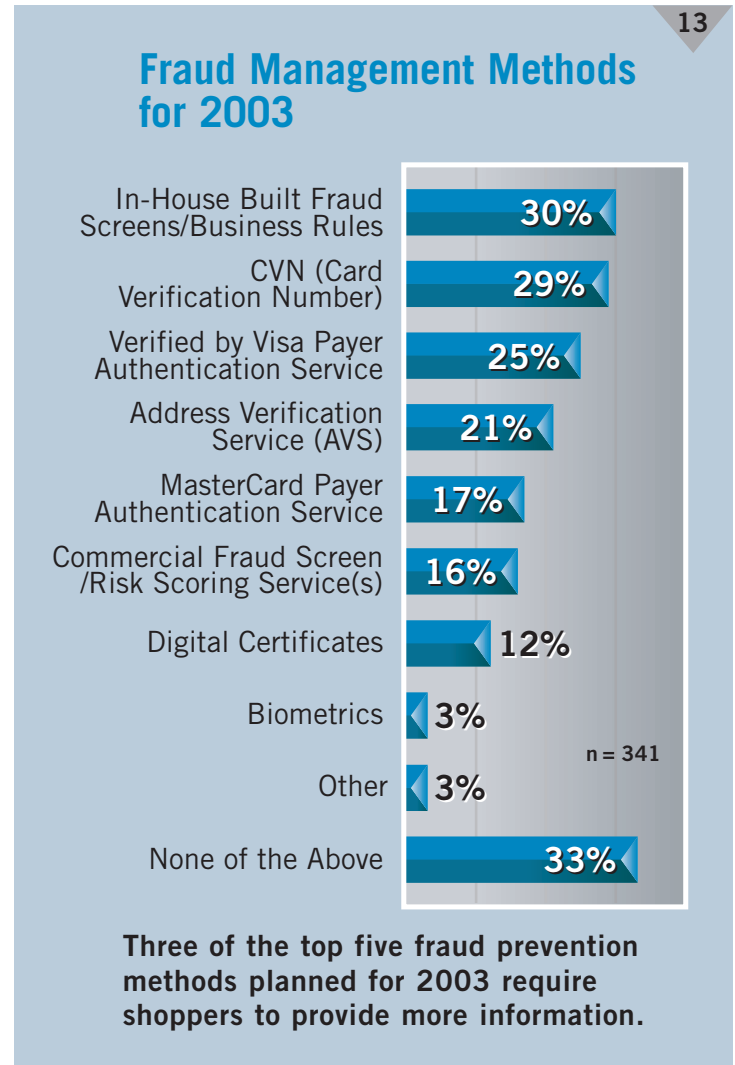
There is no single "tried-and-true" solution to the problem of managing and reducing the costs of online fraud. Just as fraudsters use a variety of ever-changing techniques to commit online credit card fraud, merchants must use a variety of methods to manage the problem in a cost-effective way. Merchants 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.

The survey results indicate that merchants are struggling to meet all of these objectives and increase their Return on Investment (ROI) for fraud-management efforts. Most merchants are employing more techniques but are not seeing significant reductions in online fraud rates or in staff time/costs. However, some merchants have achieved lower fraud rates and significant ROI for fraud management efforts by careful application of best practices to the entire order flow process (for more information, refer to the CompUSA study available from the CyberSource Web site). New fraud-management tools are now being introduced by Visa and MasterCard that present both new opportunities and online order process integration challenges, but may have significant long-term benefits in managing online fraud.

Managing Online Fraud in 2003

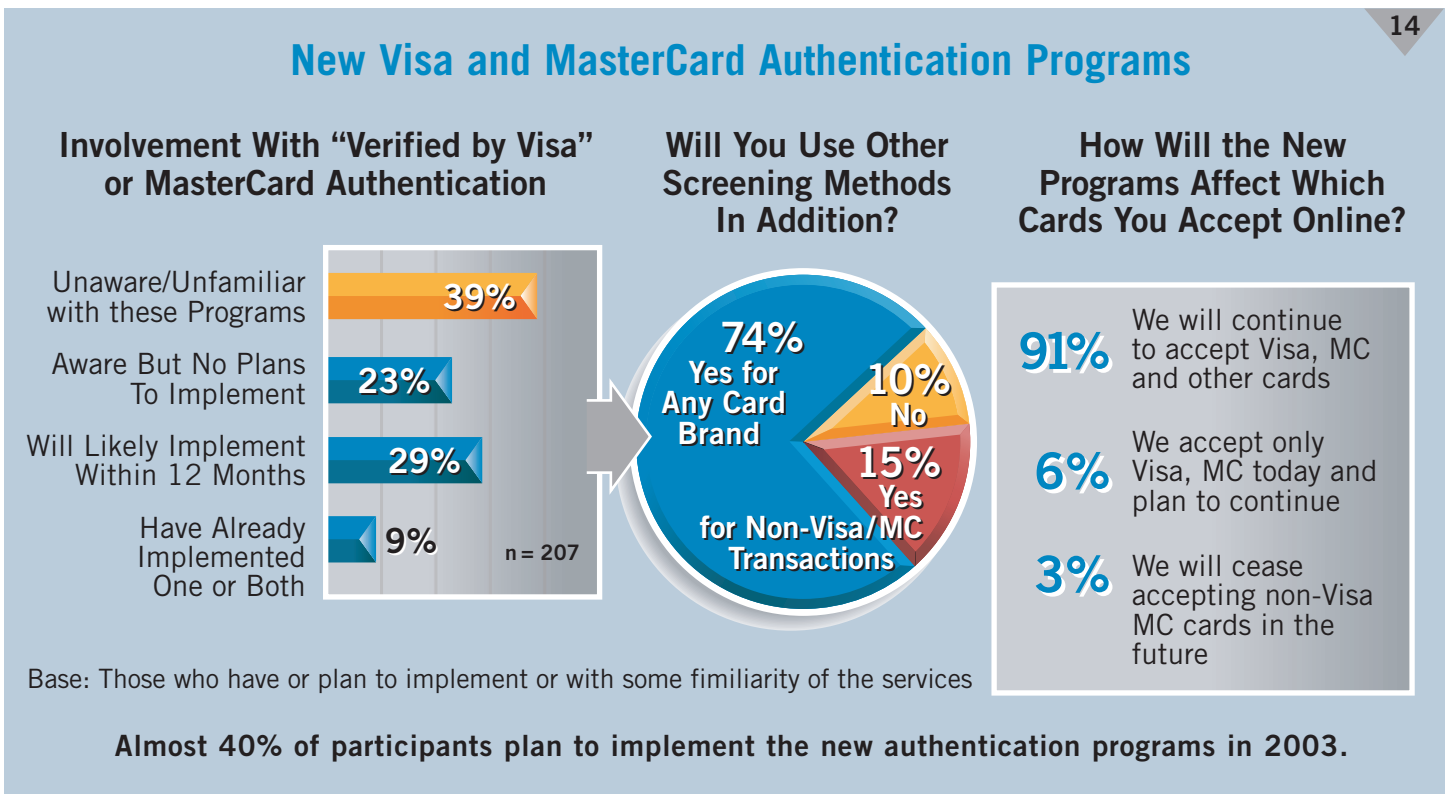
Finding: Consumers Will be Asked to Provide More Information

The survey shows that 67% of online merchants plan to adopt one or more new methods to prevent and manage online fraud in 2003. Chart 12 (below left) indicates that 43% of merchants plan to deploy two or more new methods of fraud prevention in 2003. However, many of the planned methods require additional information and involvement from the online shopper during the checkout process as shown in Chart 13 (below right).



New tools for preventing online fraud are emerging in 2003. Both Visa and MasterCard have introduced password-based systems to allow registered cardholders to authenticate their purchases. Merchants who adopt these new online checkout procedures will receive increased protection from chargeback disputes. While some merchants are not familiar with the new payer authentication systems, many already have plans to implement them in 2003. The survey shows that nearly 40% of merchants plan to implement payer authentication systems in 2003.

Chart 14 (below) shows that 23% of the merchants surveyed indicated an awareness of the new authentication tools but have opted not to implement them at this time. Some merchants have expressed concerns about the impact that the new systems will have on the online shopping experience and existing checkout processes. They are waiting to see if consumers will accept extra steps in the checkout process as well as the need for credit card passwords for online purchases.



Implementing a payer authentication system can be a complex endeavor. Before deciding whether to attempt implementation of a payer authentication system on their own, merchants need to consider the effects on their order processing and IT systems. Key considerations include system stability, decision logic and service integration, authentication request presentation to the consumer and authentication logic.

In 2003, implementation of payer authentication systems will reduce merchant liability for fraudulent credit card charges. Over the next few years, payer authentication systems should 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 is uncertain how quickly consumers will adopt these new methods of online shopping, although early indications are encouraging. It is unlikely that 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.

CyberSource Fraud Management Solutions

Efficiently managing online fraud involves integrating multiple tools and technologies to effectively minimize fraud risk, while maximizing operational efficiency and sales conversion. CyberSource's suite of modular, scalable solutions can be quickly and easily implemented as a single component or as fully-integrated systems. These modular solutions can be managed in-house, outsourced or as a blend of both options.

CyberSource Payer Authentication – Online Chargeback Protection

Our convenient, hassle-free payer authentication service gives businesses the online payment card guarantees offered by Visa and MasterCard – plus optional, additional fraud screen protection – with one easy connection. Deploy now to prepare for the payment liability rule changes due in April, 2003. This capability is also available for integration with merchants' existing systems and processes.

CyberSource Advanced Fraud Screen Enhanced by Visa – Highly Accurate Scoring

Using CyberSource technologies, highly accurate risk scores are typically calculated in under two seconds. The 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.

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, CyberSource seamlessly integrates external screening services with payment authorization and verification functions.

Additional CyberSource Products and Services – Payment, Verification and Compliance

CyberSource offers both electronic payment processing (credit cards, electronic checks, gift certificates and tax calculations) and verification and compliance solutions. These verify customer data during non-face-to-face transactions, and comply with applicable government regulations.

About CyberSource

CyberSource Corporation is a leading provider of electronic payment and risk management solutions for enterprise businesses selling via multiple sales channels. CyberSource solutions manage transaction risk and enable electronic payment processing for Web, call center/IVR, and store environments. CyberSource Professional Services designs, integrates, and optimizes enterprise-wide commerce transaction systems. More than 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 facilities 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