

CyberSource®



2017

North
America
Edition


Online
Fraud
Benchmark
Report:

Persistence
Is Critical

CyberSource is
a Visa solution



Table of Contents



Introduction	3
Survey Respondents	3
Fraud Management: A Balancing Act	4
Importance of Protecting Against Account Takeover	4
Automated Screening: Relying on the Right Set of Tools	4
Manual Review as Part of Fraud Operations	6
Managing Fraud in Different Channels	7
Accept More Genuine Orders While Guarding Against Fraud	8
Cross-Border Orders—What’s the Fraud Impact?	9
Conclusion	10
How CyberSource Can Help	10
About Us	11
Contact CyberSource	12

Introduction

Consumers continue to buy more goods and services online, increasingly with their mobile devices. Businesses recognize the imperative to accommodate these customer trends. Yet to stay competitive and retain customer loyalty, businesses must offer frictionless eCommerce and mCommerce purchasing experiences, and support the emergence of new sales channels, such as social channels.

At the same time, businesses must protect themselves and their customers from the growing threat of online fraud. Yet most businesses are forced to combat those attempts while drawing on constricted, unchanging fraud management budgets and limited resources.

The good news: Our latest survey of U.S. and Canadian businesses shows that businesses are having some success in their battle against fraud. For example, the survey results suggest businesses are succeeding in controlling losses due to fraud and even reducing the number of orders going to manual review.

Still, businesses cannot ease up on their efforts. As they continue to improve fraud detection and minimize losses,

they must also constantly strive to accept more genuine orders so they can improve the customer experience, maximize revenue, make operations as efficient as possible, and cut operational costs.

This report highlights key trends and challenges facing North American businesses and provides some insights regarding how your peers are addressing fraud. It also presents a variety of tools and approaches that can help your business ramp up fraud management efforts while increasing revenues and controlling costs.

Survey Respondents

The survey—about online, mobile, and mail order/telephone order (MOTO) fraud management practices—was conducted by Confirmit.

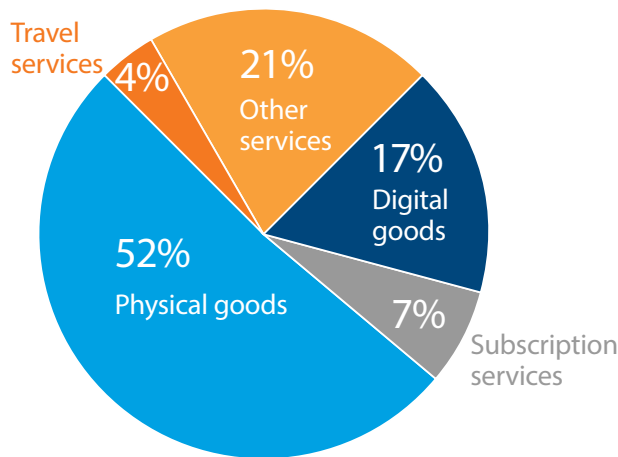
Participants:

- 466 businesses from the U.S. and Canada
- CyberSource customers and non-customers
- Representing over 12 percent of the total U.S. and Canadian eCommerce market¹

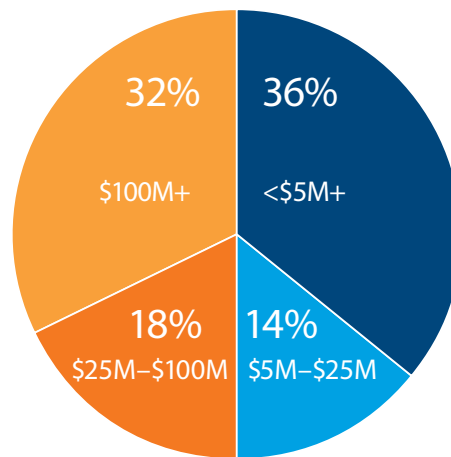
Administered:

- September–October 2016

Type of Merchant
Type of goods or services sold



Size of Merchant
Annual online revenue



¹ eMarketer 2016.

Fraud Management: A Balancing Act

Fraud management continues to be a balancing act as businesses constantly adjust their fraud strategies to minimize losses, maximize revenue, and control operational costs. This year's survey suggests that North American businesses are succeeding in controlling direct fraud loss (chargebacks plus credits issued due to fraud). Fraud losses reported by North American businesses have stabilized over the past few years. In addition, these businesses are manually reviewing fewer orders than in the past while rejecting approximately the same percentage of orders.

Still, there is important work to do. As the survey suggests, fraud teams must strive to optimize their fraud management efforts by:

- Becoming even more efficient—in particular, by more effectively managing the manual review process
- Turning away fewer genuine customers
- Streamlining fraud management across all channels

Small Fraud Management Budgets

Fraud management teams are often forced to work with very small budgets. In fact, more than half of the businesses surveyed spend less than 1 percent of their digital commerce revenue managing fraud. These results underscore the importance of maximizing the effectiveness of fraud management tools and the efficiency of operations.

Importance of Protecting Against Account Takeover

Account takeover fraud is among the top three types of fraud experienced by survey respondents. This type of fraud occurs when a fraudster exploits a customer's personal information, stored with a merchant, to take control of an existing account or establish a new one, and then uses the account to make unauthorized transactions.

Among all survey respondents, 44 percent accepted some type of recurring or subscription payment. Those businesses derive an average of 28 percent of their revenues from recurring payments. Yet only 39 percent of all survey respondents had tools in place to monitor account takeover fraud.

Automated Screening: Relying on the Right Set of Tools

Finding the right tools to automatically screen for fraud is key to achieve the right balance among minimizing losses, maximizing revenues, and controlling costs. Businesses can lower their fraud losses by deploying accurate, automated detection, and avoid unnecessary overhead by saving manual review for only the most ambiguous orders.

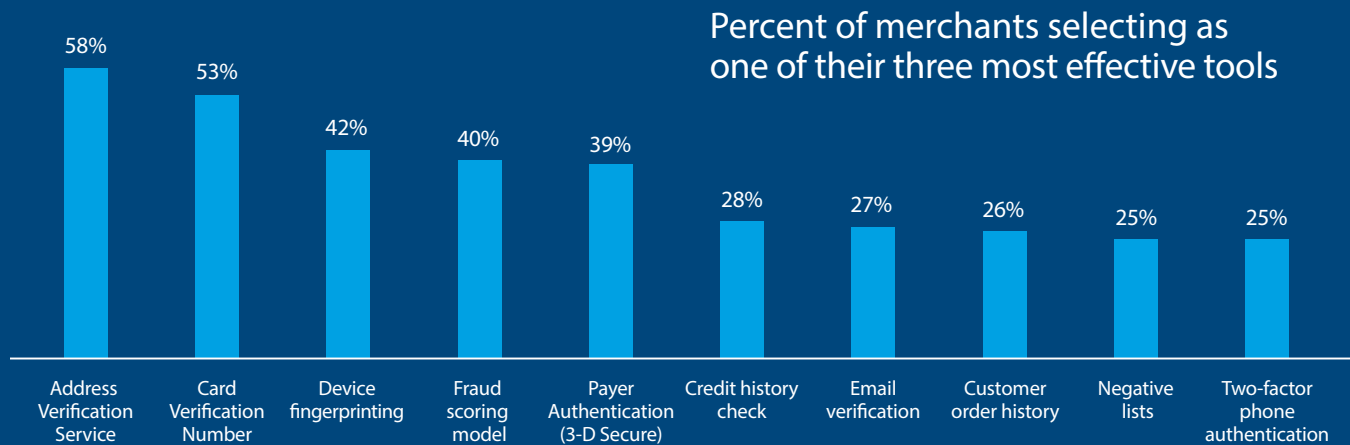
During the automated screening process, a combination of tools—including validation services, proprietary data, multi-merchant data, and device tracking—is typically applied to determine the likelihood of fraud.

Most-Adopted Fraud Detection Tools



The Most Effective Fraud Tools

Survey respondents report that some tools are more effective than others.



Identifying the Most Important KPIs

The majority of survey respondents pinpointed chargeback rate as the most important KPI for fraud management, followed by various versions of fraud rates.

1. Chargeback rate (62 percent)*
2. Fraud rate by value (47 percent)*
3. Confirmed fraud rate (35 percent)*
4. Fraud rate—order volume (27 percent)*

* Percent of respondents who selected this KPI as one of their top three

Manual Review as Part of Fraud Operations

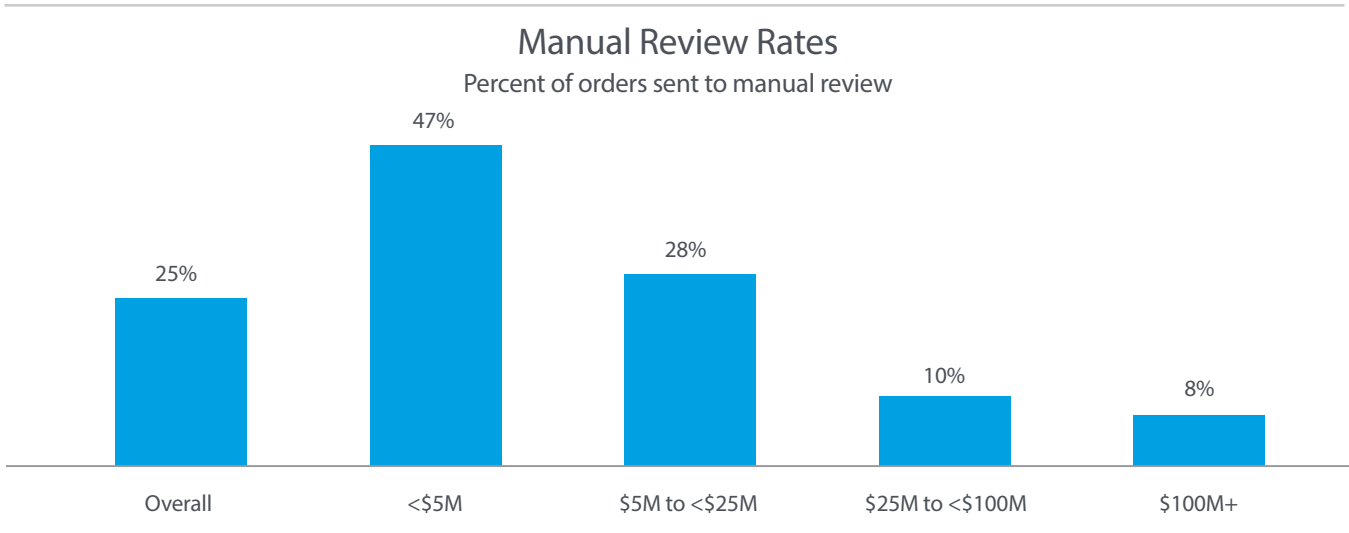
Manual Review Is Helpful, But Can Be Costly

Manual review remains prevalent:

- Seventy-nine percent of North American businesses conduct manual reviews.
- On average, these businesses manually review 25 percent of orders.

However, manual review is often a costly aspect of fraud management operations, frequently constituting a large part of the fraud management budget.

According to survey results, businesses accepted 89 percent of orders following manual review—an indicator that more orders are being reviewed than might be necessary. Automated screening can make your fraud management processes more efficient for most orders while leaving only the most suspect ones to be reviewed manually by your team.



Managing Fraud in Different Channels

Businesses Track Fraud Across Channels

Of those businesses surveyed, 74 percent track fraud losses in their web store, and 49 percent in their mobile channel. Businesses that track fraud by order channel are better able to implement channel-specific fraud strategies for the channels they sell through.

mCommerce in the Spotlight

mCommerce appears to be on the rise. For the respondents who track this information, the percentage of revenue originating from mobile devices—including orders placed through a mobile-optimized website or a mobile app, but not including mobile point-of-sale (mPOS) sales—increased from 25 percent in 2015 to 33 percent in 2017.

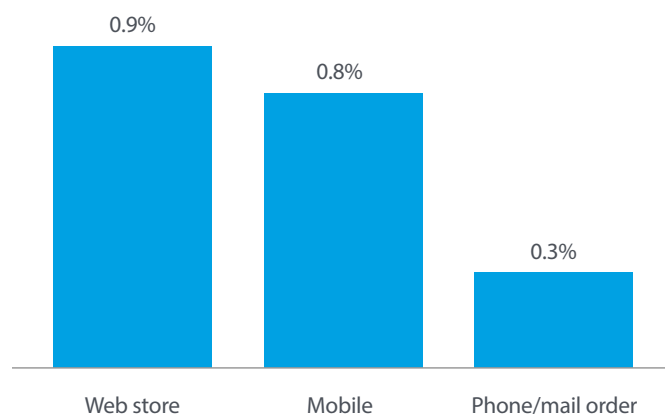
Managing Mobile Fraud

Distinguishing mCommerce from eCommerce, and tracking fraud in each channel separately, is critical to reducing fraud in the mobile channel and minimizing the number of good mCommerce transactions you need to review and reject. In assessing mCommerce transactions, you can use all of the captured order information—such as the channel, time of day, customer identity, and item purchased—as input to establish fraud rules. The more relevant data there is, the more that can be done to distinguish genuine orders from fraudulent transactions.

91% of businesses use the same fraud management tools for mobile and web channels.

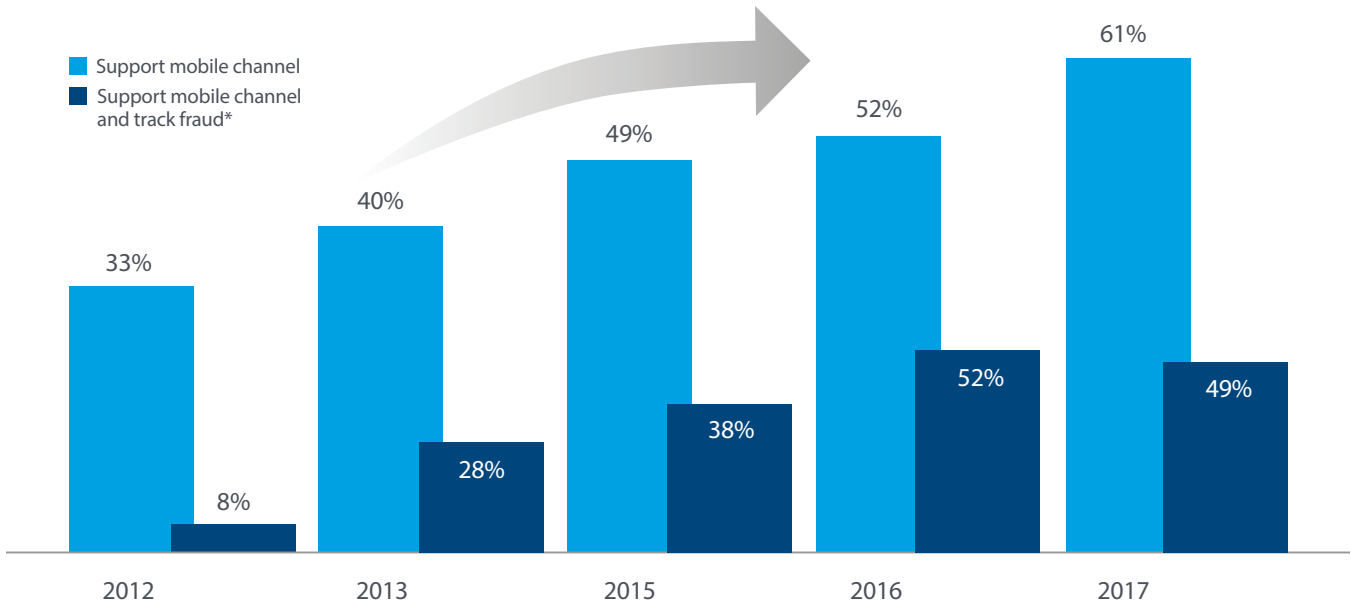
Overall Fraud Loss by Order Channel

Reported average annual fraud loss
(Expressed as percent of annual eCommerce revenue)



Q: For each channel, what percent of your annual eCommerce revenue do you expect to lose due to payment fraud?

Growth and Tracking of the Mobile Channel



*Percent of businesses surveyed that indicated they have a mobile channel and track fraud loss rates in that channel

Accept More Genuine Orders While Guarding Against Fraud

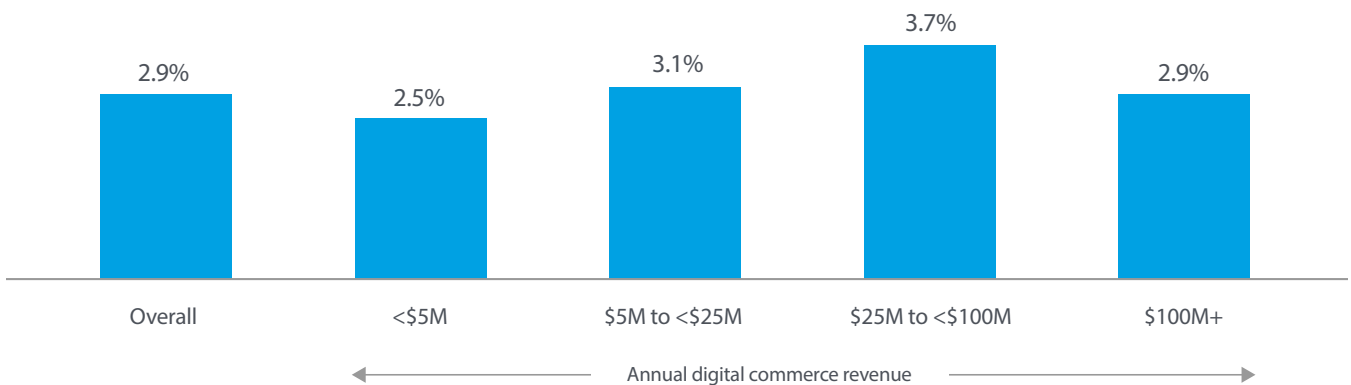
Rejection Rates and False Positives

North American businesses rejected 2.9 percent of U.S./Canadian orders due to suspicion of fraud, similar to the 2016 level of 2.8 percent.

A false positive (customer insult) is created when a fraud management process rejects a valid customer's order, treating it as attempted fraud. False positives result in immediate lost sales—and they can affect customer loyalty, retention, and future sales. It is often difficult to track false positives. Yet 68 percent of survey respondents attempt to track false positives, and they believe that up to 10 percent of their rejected orders were actually genuine.

Order Rejection Trends by Size of Merchant

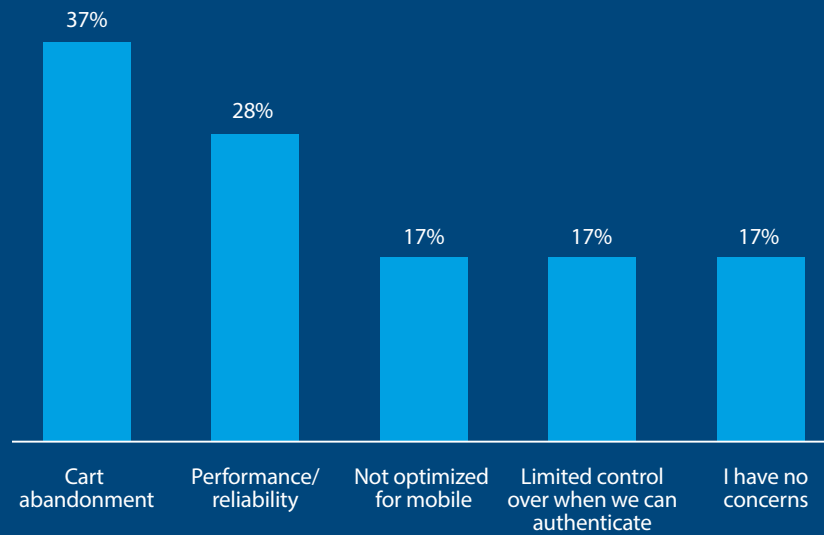
Percent of orders rejected



Increasing Genuine Order Acceptance with 3-D Secure

Implementing payer authentication (3-D Secure) can help you accept more genuine orders but also can lead to shopping cart abandonment. Still, according to the survey, 49 percent of respondents were concerned about 3-D Secure creating customer friction, and 18 percent did not implement 3-D Secure for that reason. Thirty-seven percent of respondents specifically were concerned that 3-D Secure could result in cart abandonment with 13 percent not implementing the technology for that reason.

Merchant Challenges with Standard 3-D Secure



The situation might change with the 3-D Secure 2.0 specification released by EMVCo in 2016. This new specification will better reflect current and future market requirements for digital payments beyond traditional browser-based eCommerce transactions, and support app- and device-based authentication. The technology will also improve the consumer experience by enabling intelligent, risk-based decisioning and frictionless consumer authentication.

Cross-Border Orders—What's the Fraud Impact?

Despite the challenges of managing cross-border fraud, many North American businesses are successfully managing their fraud risks when handling these international transactions. However, there remains a significant difference in the order rejection rate between cross-border and domestic orders: The order rejection rate for cross-border orders is over twice the rate of domestic orders.

Working with a Global Partner

If you are moving into new geographies, consider:

- Working with local fraud management experts knowledgeable in each market you consider entering
- Implementing regionally relevant best practices
- Adjusting fraud scoring rules to reflect local markets

- **54% of survey respondents accept orders from outside North America**
- **16% of orders accepted are cross-border transactions**

eCommerce Fraud Loss Rate

Domestic versus cross-border

- Percent of domestic orders that were fraudulent
- Percent of cross-border orders that were fraudulent

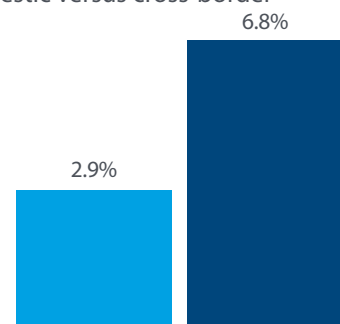


2017

Order Reject Rate

Domestic versus cross-border

- Percent of domestic orders rejected due to suspicion of fraud
- Percent of cross-border orders rejected due to suspicion of fraud



2017

Conclusion

The North American businesses in our survey are managing fraud reasonably well. But they can't afford to let up on their fraud management efforts. In addition to enhancing fraud detection and avoiding the losses caused by fraud, they must work to boost revenue by accepting the maximum number of good orders. At the same time, they must also enhance the efficiency of fraud management so they can keep operational costs under control.

As the survey shows, manual review continues to be one of the more expensive, time-consuming components of fraud management. While manual review can provide additional insight, overreliance on manual review can prove costly. Implementing tools that enhance the accuracy of automated fraud screening can help many businesses overcome the hurdles of manual review. These tools can help conserve manual review resources, reserving the manual review process for a smaller number of orders.

Overall, fraud management continues to present serious challenges for businesses navigating an increasingly complex and competitive digital economy. However, with the right tools, your business can effectively address those challenges and reduce fraud losses while minimizing operational costs and improving the customer experience.

How CyberSource Can Help

The digital economy continues to evolve, requiring many businesses to reassess their fraud management processes. As customers engage with you across multiple channels, using a variety of devices, you need a holistic approach to fraud. CyberSource can help you implement that approach, providing a complete range of fraud management solutions that enable you to identify fraud faster, more accurately, and with less manual intervention. Here are some of these solutions.

CyberSource Enterprise Fraud Management

CyberSource Enterprise Fraud Management is a multi-stage fraud management solution that spans account monitoring, transaction fraud detection, rules tuning, and payer authentication. Accept more good orders, streamline operations, and gain agility. Fine-tune screening models and strategies—regardless of whether based on relationships—or stretch across multiple channels, various devices, or different levels of service.

Decision Manager

Automate and streamline your fraud operations with CyberSource Decision Manager—the only fraud management platform that features the World's Largest Fraud Detection Radar, which includes insights drawn from the more than 68 billion transactions processed by Visa and CyberSource. Take advantage of a flexible rules engine to customize rules and models to your specific business across all sales channels, including web, mobile, call center, and kiosk channels. Optimize fraud processes by using Real-Time Fusion Modeling technology that blends multiple advanced machine-learning methods for accurate scoring.

Decision Manager Replay

CyberSource Decision Manager Replay lets you confidently quantify the impact of your rule changes in real time, before activating them in your live production environment. An industry first, Decision Manager Replay lets you immediately compare various “what-if” rules profiles against your own historical data, rather than waiting months to understand the impact of fraud changes. Decision Manager Replay produces real-time insights into likely changes to the transaction disposition and fraud rates before you push rules changes live.

Rules-Based Payer Authentication

Working with CardinalCommerce, CyberSource Rules-Based Payer Authentication provides you with control over the customer experience along with all the benefits of traditional 3-D Secure, including the liability shift and reduction of interchange fees. You decide when to request payer authentication protection so you can guard against fraud and deliver more seamless checkout experiences for your customers.

Account Takeover Protection

Account takeover fraud is an increasingly prevalent type of online threat that occurs when a fraudster exploits a victim’s personal information to take control of an existing account or establish a new account. The fraudster then uses the account to carry out unauthorized transactions.

CyberSource Account Takeover Protection defends customers and merchants from fraudulent uses of online accounts. It helps identify high-risk users at account creation and login, and monitors for suspicious account changes. With Account Takeover Protection, you can keep your customer accounts safe and protect against fraudulent card-on-file payments while streamlining access for authenticated customers.

Loyalty Fraud

CyberSource fraud management can also help you provide a more secure online environment for loyalty program customers. Guard against fraud throughout the loyalty lifecycle, including purchase and redemption of points as well as account creation, login, and account updates. The CyberSource loyalty fraud management solution combines advanced analytical algorithms, customizable rules, data from approximately 68 billion transactions, and global expertise to optimize the accuracy of your fraud screening. With experience protecting loyalty points and miles as a currency, CyberSource can help you reduce loyalty program risk.

Managed Risk Services

Complement your in-house skills and resources with the global team of CyberSource fraud management experts. Managed risk analysts who serve clients on six continents can help you optimize CyberSource Decision Manager results and scale operations. This global knowledge network helps identify new fraud trends before they affect your business. Count on CyberSource to be your trusted partner as your business expands.

About Us

CyberSource Corporation, a wholly owned subsidiary of Visa, Inc., is a global payment management platform. More than 465,000 businesses worldwide use CyberSource and Authorize.Net brand solutions to process online payments, streamline fraud management, and simplify payment security. For more information, please visit www.cybersource.com.



For more information visit www.cybersource.com/products/fraud_management

CyberSource, a wholly owned subsidiary of Visa, Inc., is the only integrated payment management platform built on secure Visa infrastructure, with the payment reach and fraud insights of a massive \$358 billion global processing network. CyberSource and Authorize.Net payment management solutions help 465,000 large and small businesses worldwide grow sales, mitigate risk, and operate with greater agility. For more information, please visit www.cybersource.com

CyberSource®

CyberSource is
a Visa solution

VISA