VISA

Online Fraud Report

2017 Latin America

CyberSource®

eCommerce Institute
de Latinoamérica al Mundo

Table of Contents

 © Copyright 1996-2017. All Rights Reserved.

Introduction

Merchants continue to expand into new channels and markets to meet customers' demand for eCommerce, while at the same time fraud increases. Visa commissioned an annual report of Latin America and the Caribbean businesses to advance the industry's management of online fraud and business operations, and take an in-depth look at the online and mobile fraud landscape.

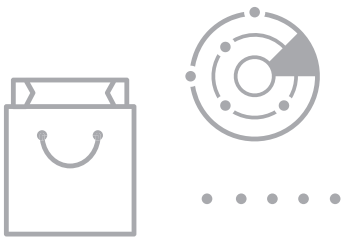
Customers continue to buy more goods and services online, increasingly with their mobile devices. Yet to stay competitive and retain customer loyalty, businesses must offer frictionless eCommerce and mCommerce purchasing experiences, and support the emergence of new sales channels.

At the same time, businesses must protect themselves and their customers from the growing threat of online fraud. Today most merchants must deal with constricted, unchanging fraud management budgets and resources.

Nonetheless, merchants cannot ease up on their efforts to continue to improve fraud detection and minimize losses. They must focus on accepting more good orders while balancing between improving the customer experience, maximizing revenue, making their fraud operations as efficient as possible, and working to reduce operational costs.

This report highlights key trends and challenges facing Latin American and Caribbean businesses and provides some insights regarding how to fight 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.

Visa Merchant Sales & Solutions

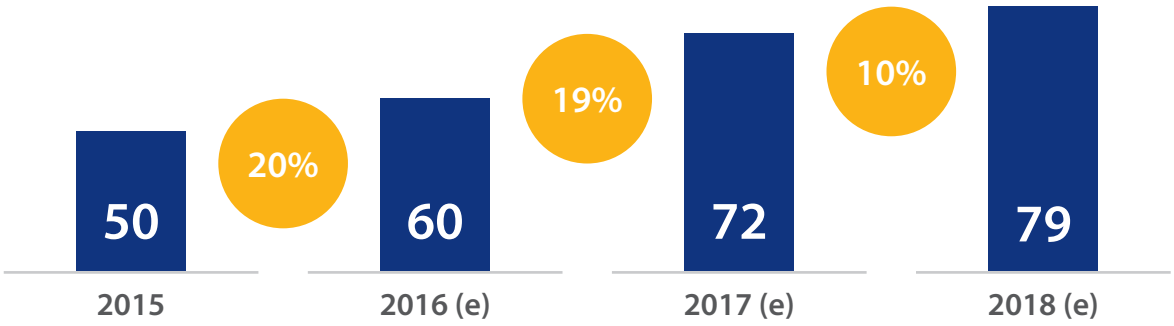


© Copyright 1996-2017. All Rights Reserved.

eCommerce in Latin America

Online Sales in Latin America are expected to reach **US$72 Billion** in 2017 (e)[1]

eCommerce Growth Rate in Latin America (US$ B) (e)[1]



Latin America eCommerce Sales by Market (e)[1]

1. E-readiness in Latin America 2016, a Visa study commissioned to Euromonitor International.
2. Remaining countries in Latin America & the Caribbean

 © Copyright 1996-2017. All Rights Reserved.

Survey Methodology

This study measured key fraud management trends and best practices across a sample of Latin America and Caribbean small, medium and large companies.

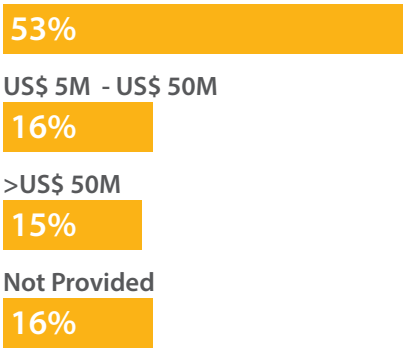
Respondents to this survey reported information from the 2016 calendar year. Survey respondents were actively involved in their organizations' fraud management policies and eCommerce operations. **266** survey respondents, comprising both CyberSource customers and non-CyberSource customers, completed the online questionnaire between March and June 2017. Independent market research firm Confirm-it conducted the survey.

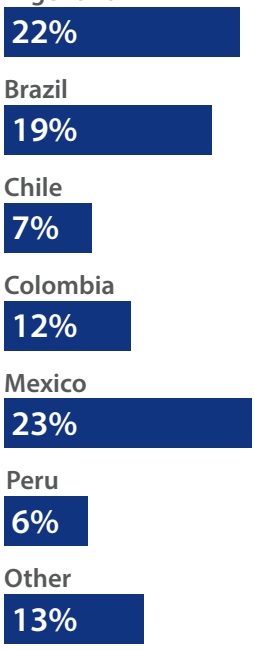
Respondents by

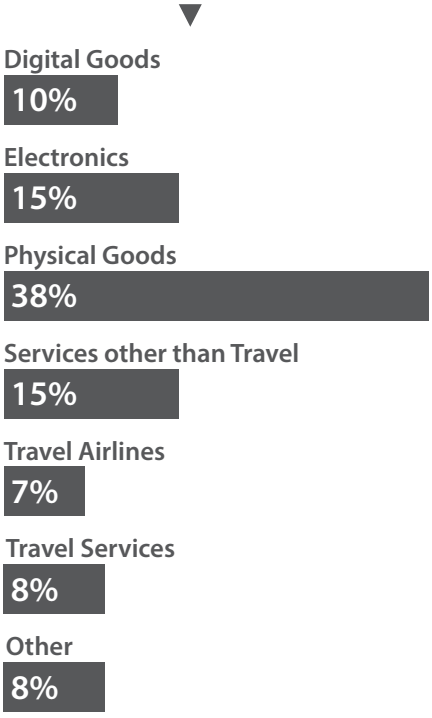
Online Size by Annual Sales

Country Where Headquarters are Located

Industry







© Copyright 1996-2017. All Rights Reserved.

Executive Summary

Latin America and the Caribbean comprise one of the fastest growing eCommerce markets in the world, with sales expected to reach **US$ 72 Billion** by 2017[1]. This rapid rise in eCommerce across multiple channels goes hand-in-hand with higher fraud rates, making it mission-critical for businesses to implement efficient and effective fraud management strategies.

Developing a fraud management plan is a balancing act unique to each business. It requires navigating the tradeoffs among reducing fraud losses, maximizing revenue, and minimizing operational costs. This **2017 Online Fraud Report for Latin America** reveals how businesses are currently managing digital fraud by analyzing key metrics including chargeback rates, order rejection and manual review.

It is clear that while many merchants have fraud management tools in place, there is much room for improvement. Currently Latin American and Caribbean merchants reported a chargeback rate of **1.7%[2]**, a manual review rate of **28%[2]**, and a rejection rate of **9.2%[2]**. This means that businesses are potentially sacrificing a significant portion of valid orders, thereby alienating good customers and reducing potential revenue.

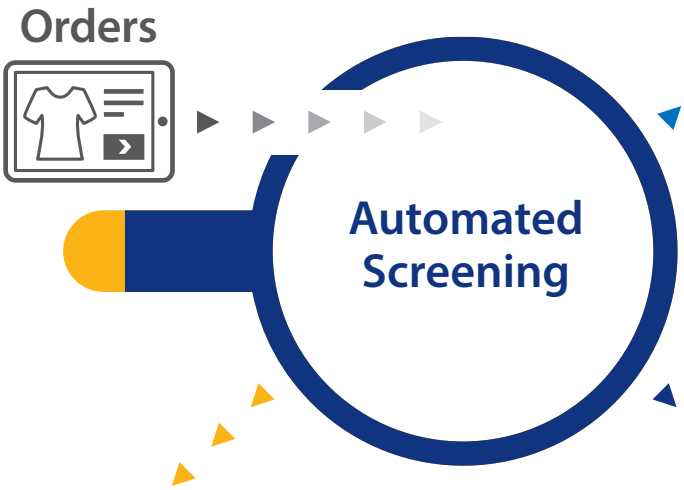
Adding another layer of complexity is detecting fraud in the rapidly growing mCommerce channel which is expected to more than triple from 2015 to 2020 to **US$ 16.6 Billion[3]**. While **67%[2]** of Latin American and Caribbean merchants report that they screen for fraud in the mobile channel, the methods they use are typically the same as those used for eCommerce and are not tailored to accurately detect mobile fraud. Distinguishing mCommerce from eCommerce, and tracking fraud in each channel separately, is critical to reducing fraud in the mobile channel. That way Latin American and Caribbean merchants can implement effective mobile fraud detection tools to incorporate into their overall fraud management strategies.

By understanding your own fraud metrics and your various business tradeoffs, you can use the findings in this report to benchmark your performance and discover areas to improve your fraud management strategies. As digital commerce in Latin America and the Caribbean continues to grow across channels, businesses with optimized fraud management strategies will be able to take advantage of these growing opportunities while mitigating fraud risks.

1. E-readiness in Latin America 2016, a Visa study commissioned to Euromonitor International.
2. 2017 Online Fraud Report for Latin America
3. Euromonitor International 2015

 © Copyright 1996-2017. All Rights Reserved.

The Risk Management Pipeline™ Framework



9.2% of orders are **rejected** due to suspicion of fraud in Latin America

Argentina	6.3%
Brazil	7.6%
Colombia	8.1%
Mexico	14.3%
Others[1]	7.4%
Latin America	9.2%
US and Canada[2]	2.9%

82% of merchants conduct **manual review** in Latin America

Argentina	83%
Brazil	86%
Colombia	86%
Mexico	86%
Others[1]	76%
Latin America	82%
US and Canada[2]	79%

28% of the orders are **reviewed manually**

Argentina	37%
Brazil	20%
Colombia	24%
Mexico	25%
Others[1]	32%
Latin America	28%
US and Canada[2]	25%

57% of manually reviewed orders are ultimately **accepted**

Argentina	67%
Brazil	56%
Colombia	67%
Mexico	50%
Others[1]	55%
Latin America	57%
US and Canada[2]	89%

1.7% of sales become **chargebacks**

Argentina	1.2%
Brazil	1.6%
Colombia	1.5%
Mexico	2.2%
Others[1]	1.5%
Latin America	1.7%

1. Remaining countries in Latin America and the Caribbean.
2. 2017 North America Online Fraud Benchmark Report, CyberSource.

© Copyright 1996-2017. All Rights Reserved.

Automated Screening

Finding the right tools to automatically screen fraud is a key part of achieving a balance.

A company can keep fraud low 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 in Latin America

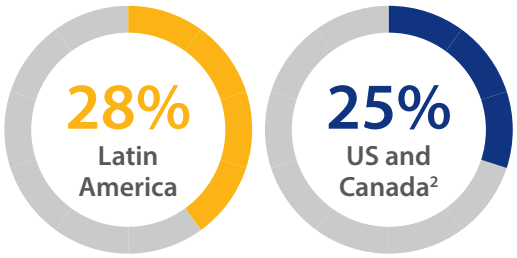
- Card Verification Number (CVN)
- Credit history check
- Customer order history
- Device fingerprinting
- Email verification
- Fraud scoring model (company - specific)
- Geographic indicators/maps
- Geolocation information (country, city, etc.)
- Negative list/blacklists (in-house lists)
- Paid-for public records services
- Payer Authentication (3-D Secure)
- Proxy detection
- Search engine results
- Shared negative lists - shared hotlists
- Social networking sites
- Positive lists/whitelists
- Two-factor phone authentication (in-app, SMS, email)
- Velocity test

 © Copyright 1996-2017. All Rights Reserved.

The Cost of Fraud Operations: Manual Review

Manual Review Rate

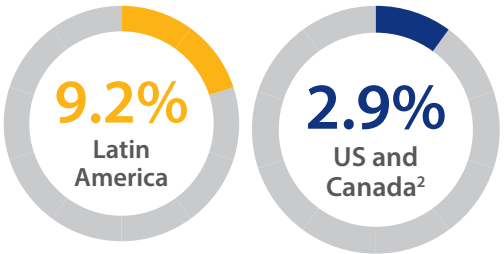
37% Argentina | 20% Brazil | 24% Colombia | 25% Mexico | 32% Others[1]



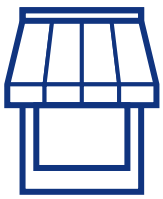
Improve Order Acceptance Rates

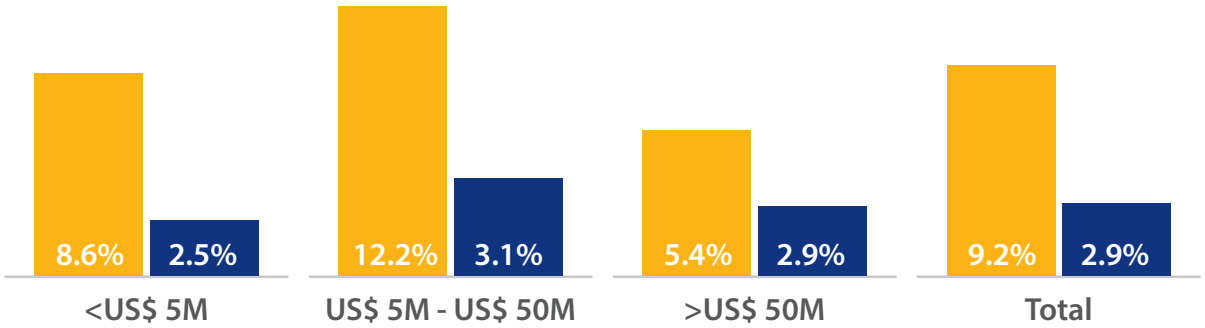
Rejected Orders due to Suspicion of Fraud

6.3% Argentina | 7.6% Brazil | 8.1% Colombia | 14.3% Mexico | 7.4% Others[1]



Rejected Orders by Merchant Size



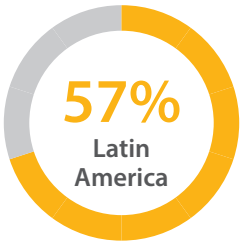


1. Remaining countries in Latin America and the Caribbean
2. 2017 North America Online Fraud Benchmark Report, CyberSource.

© Copyright 1996-2017. All Rights Reserved.

Post-Review Accepted Orders

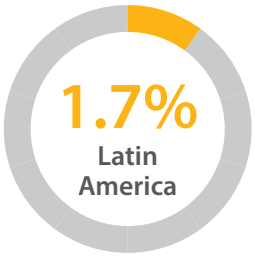
67% Argentina | 56% Brazil | 67% Colombia | 50% Mexico | 55% Others[1]



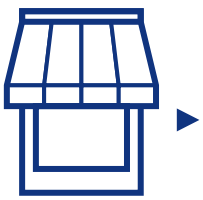
Chargebacks (Fraud Claim Management)

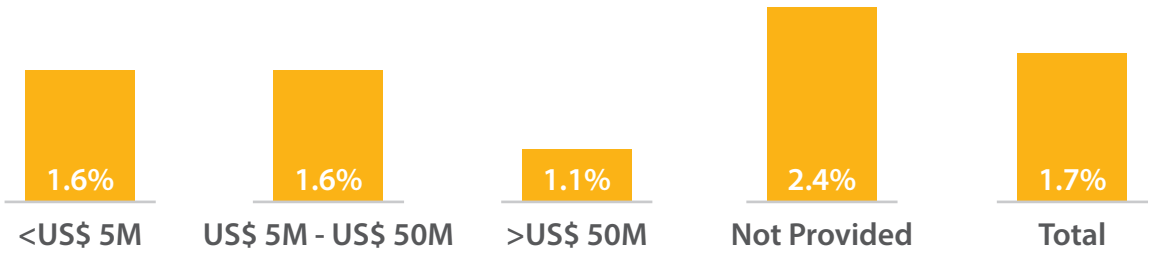
Chargeback Rate by Revenue

1.2% Argentina | 1.6% Brazil | 1.5% Colombia | 2.2% Mexico | 1.5% Others[1]



Chargeback Rate by Revenue and Merchant Size (Annual)





1. Remaining countries in Latin America and the Caribbean
2. 2017 North America Online Fraud Benchmark Report, CyberSource.

Latin America

 © Copyright 1996-2017. All Rights Reserved.

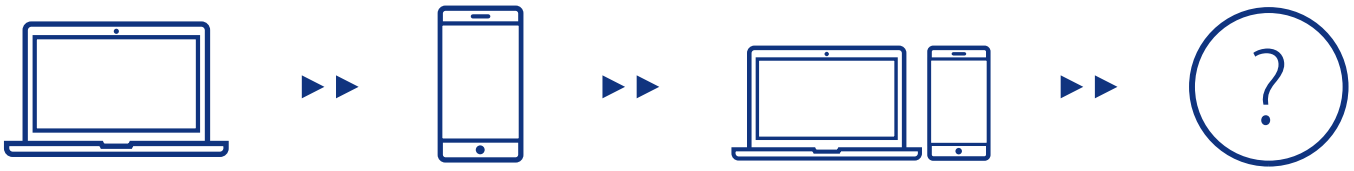
Mobile Commerce and Fraud Prevention in Latin America

The rise of mobile, and smartphones in particularly, has driven online commerce from an "anytime" experience to an "anytime, anywhere" experience.

As the online and physical worlds converge, mobile is the bridge, providing consumers access to online services in the Face To Face (F2F) environment and seamless commerce experiences. Mobile empowers the consumer, driving expectations for personalized experiences and outcomes delivered in a seamless way.

Here are some statistics from our 2017 Online Fraud Management survey for Latin America and the Caribbean.

Merchants Operating Through Mobile Channels



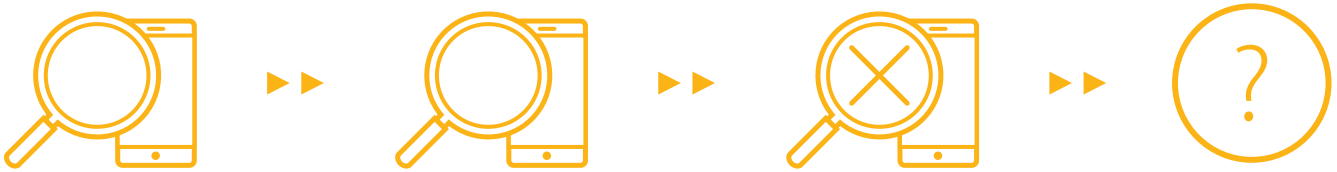
53%
Mobile Commerce Website

7%
App

31%
Mobile Commerce Website & App

9%
Do Not Know

Fraud Prevention Strategy for Mobile Channels



45%
Yes, We Screen with eCommerce Fraud Management Tools

22%
Yes, We Screen with Other Fraud Management Tools

29%
We Do Not Use a Fraud Management Tool in Mobile Channels

4%
Do Not Know

© Copyright 1996-2017. All Rights Reserved.

Global Online Fraud Indicators – 2017

Linear Averages

	Chargeback Rate by Revenue	Rejected Orders	Manual Review Rate	Reviewed Orders	Orders Accepted Post Manual Review
Argentina	1.2%	6.3%	83%	37%	67%
Brazil	1.6%	7.6%	86%	20%	56%
Colombia	1.5%	8.1%	86%	24%	67%
Mexico	2.2%	14.3%	86%	25%	50%
Others[1]	1.5%	7.4%	76%	32%	55%
Latin America	1.7%	9.2%	82%	28%	57%
US and Canada[2]	-	2.9%	79%	25%	89%

1. Remaining countries in Latin America and the Caribbean
2. 2017 North America Online Fraud Benchmark Report, CyberSource.

 © Copyright 1996-2017. All Rights Reserved.

Conclusion

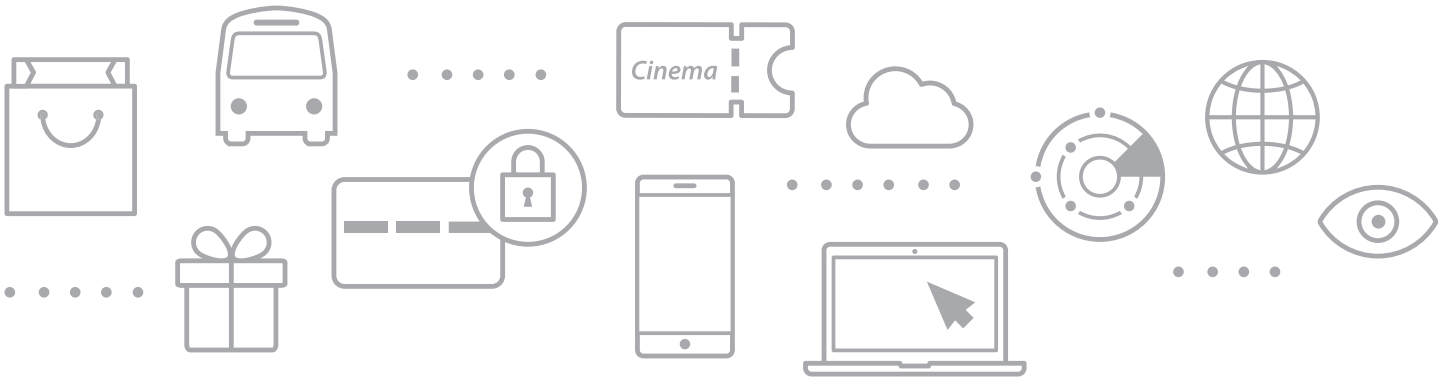
Latin American and Caribbean businesses have an enormous opportunity for revenue growth due to rapidly expanding eCommerce – an opportunity that is combined with greater risks and costs associated with digital fraud.

The proliferation of sophisticated techniques used by fraudsters requires businesses to arm themselves with ever-more powerful fraud management tools.

Currently businesses rely heavily on manual review, which is labor-intensive, time-consuming, and bring potential for human error. Automated detection tools that screen orders in real-time to correctly distinguish genuine versus fraudulent purchases can help increase revenue, improve operational efficiency and reduce fraud costs – with the added benefit of streamlining order acceptance and improving the customer experience.

This is especially critical for mid-size companies that may have invested less in automated fraud tools than large companies. Fraudsters tend to migrate to businesses that have less accurate detection programs in place. Mid-size companies face even greater risks of increased fraud costs as perpetrators target companies where they are less likely to be detected.

We hope this report has helped your company benchmark fraud management practices, track fraud indicator metrics, including fraud rates, chargebacks, and manual review rates, so you can develop new ways to improve your overall fraud management strategies. As digital commerce continues to grow across channels, only those businesses that successfully mitigate fraud risk will be able to take full advantage of the increased eCommerce opportunities.



© Copyright 1996-2017. All Rights Reserved.

How Visa 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 to consider a holistic approach to fraud management. CyberSource can help you by 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 those solutions.

CyberSource Enterprise Fraud Management

CyberSource Enterprise Fraud Management is a multi-layered fraud management solution – from account monitoring to transaction fraud detection, to rules-tuning, to payer authentication – that helps businesses minimize fraud losses, maximize revenue and minimize operational costs. Fine-tune screening models and strategies—regardless of whether based on relationships—that 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 rules changes. Decision Manager Replay produces real-time insights into likely changes to the transaction disposition and fraud rates before you implement 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 Management

Loyalty fraud is a growing challenge in the digital economy as businesses seek to increase their volume of repeat customers through loyalty and reward programs. The CyberSource Loyalty Fraud Management solution can help protect your business and your customers by accurately diagnosing fraudulent behaviors throughout the loyalty lifecycle and provide a more secure online environment for your loyalty program customers.

Guard against fraud throughout the loyalty lifecycle, including orders 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 consultants across five 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.

 © Copyright 1996-2017. All Rights Reserved.

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

Latin America and the Caribbean
lac@cybersource.com

mexico@cybersource.com

brasil@cybersource.com

US and Canada
sales@cybersource.com

Europe
uk@cybersource.com

Japan
sales@cybersource.co.jp

Asia Pacific
ap_enquiries@cybersource.com