CyberSource®

Payment Management for the Digital Economy

ANNUAL FRAUD BENCHMARK REPORT: A BALANCING ACT

NORTH AMERICA EDITION 2016

CyberSource is part of Visa

VISA

TABLE OF CONTENTS

INTRODUCTION

If there's one word that sums up the way the world is changing when it comes to managing fraud across digital channels, it's "more." More people are buying more goods and services online. That means more opportunity for businesses, but also more competition — and more demanding customers.

There's more commerce being conducted over mobile devices — the mobile channel is growing at a rapid pace as use of smart devices continues to rise. And there are more channels beyond mobile, with every social network now a potential point of sale.

Naturally, this expanding digital commerce environment attracts more fraudsters attempting more fraud — often in more sophisticated ways — across all selling channels.

For fraud management teams, this means a more complex operating environment than ever before. But this complexity doesn't usually come with more budget to fight fraud or less pressure to deliver results.

A BALANCING ACT

Our latest survey of U.S. and Canadian businesses shows that, despite all this complexity, fraud management teams are successfully managing fraud, with revenue lost to eCommerce fraud remaining relatively stable over the past five years.

But to optimize fraud management, you need to balance lowering fraud losses against:

- Accepting more genuine orders to maximize revenue
- Making your operations as efficient as possible to minimize operational costs

Based on the results of the survey, we look at key trends and challenges facing North American businesses seeking to find the right balance and discuss some of the approaches and tools that are available to help you.

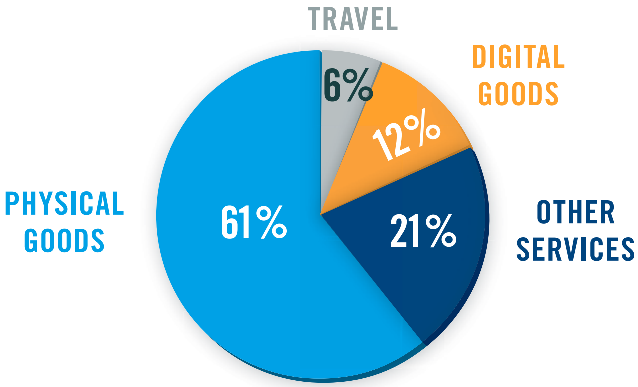
WHO DID WE ASK?

A survey about online, mobile, and MOTO fraud management practices was conducted by Confirmit®. 307 North American businesses in the U.S. and Canada participated in the study.

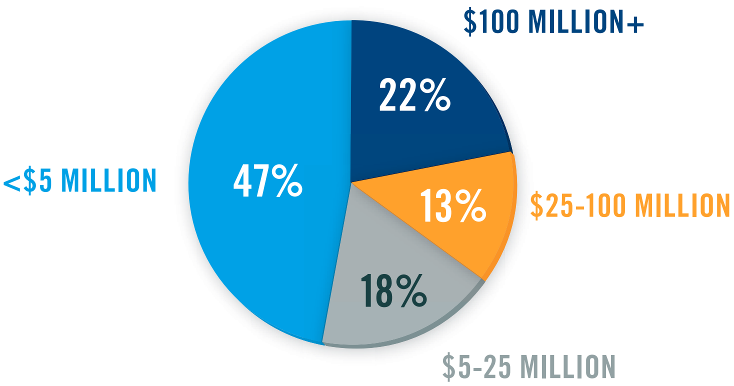
The survey was carried out between October and November 2015 and reflects merchant reported annual payment fraud metrics, inclusive of chargebacks and credits issued due to fraud, across all payment types.

Respondents were comprised of both CyberSource customers and non-customers, representing over $137 billion in combined online revenue. This report summarizes the survey findings.

TYPE OF MERCHANT



SIZE OF MERCHANT
(ANNUAL ONLINE REVENUE)



CyberSource®

CyberSource is part of Visa VISA

THE BALANCING ACT

Fraud management is a balancing act. Businesses need to constantly adjust their strategy to minimize fraud losses, maximize revenue, and minimize operational costs.

The good news is that North American businesses have succeeded in controlling direct fraud loss (chargebacks plus credits issued due to fraud). But that achievement comes at a cost, because they are:

- Manually reviewing more orders
- Rejecting more orders

Fraud teams are looking to optimize their operations by:

- Being more efficient — in particular, by cutting the cost of manual review
- Turning away fewer genuine customers
- Further streamlining fraud management across all channels

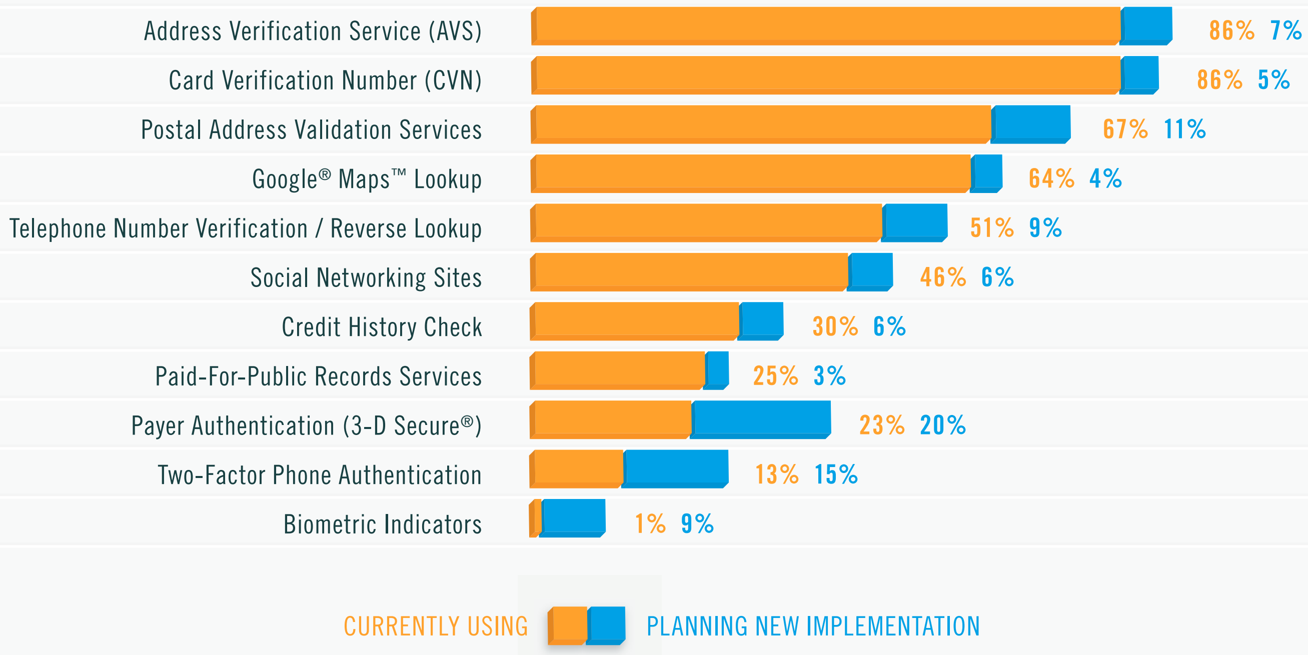
AUTOMATED SCREENING: THE MOST ADOPTED FRAUD DETECTION TOOLS

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

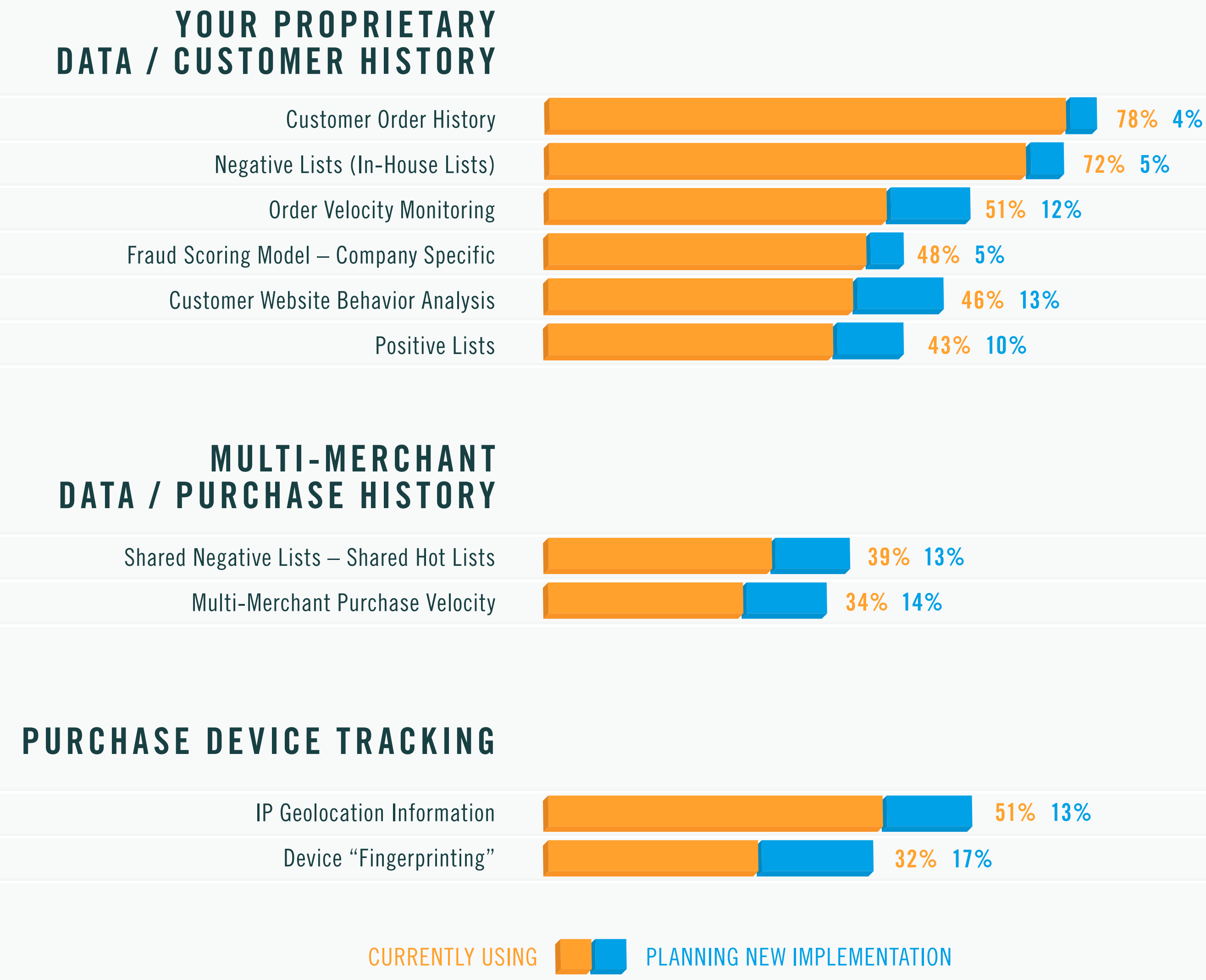
During the automated screening process, a combination of tools — including validation services, proprietary data, multi-merchant data, and device tracking — is typically applied to determine the likelihood of fraud.

MOST ADOPTED FRAUD DETECTION TOOLS

VALIDATION SERVICES



MOST ADOPTED FRAUD DETECTION TOOLS



VALIDATION SERVICES

Among validation services, address verification service (AVS) and card verification number (CVN) are the top two tools used to identify fraudulent transactions.

PROPRIETARY AND MULTI-MERCHANT DATA

Customer order history is still the most relied-on type of proprietary data, while use of multi-merchant data, including shared negatives lists and multi-merchant purchase velocity, has also increased.

PURCHASE DEVICE TRACKING

Actual and planned adoption of device fingerprinting has increased. This may be because more businesses now have, or intend to launch, a mobile sales channel.

THE COST OF FRAUD OPERATIONS: MANUAL REVIEW

ASSESSING THE IMPACT OF NEW STRATEGIES BEFORE TURNING THEM LIVE

When changing customer or fraudster behavior patterns requires new or revised rules in an automated screening tool, it typically takes several months before you can properly assess their impact on fraud reduction and revenue capture.

CyberSource Decision Manager Replay eliminates that time lag. It lets you quickly test and quantify the expected impact of new fraud management strategies on historical transactions — and see the projected results in minutes.

By comparing and reporting on fraud rule profiles, your fraud analysts can quickly evaluate the business outcomes of various fraud management strategies (orders accepted, rejected, and sent to manual review) before choosing which to activate in the production environment.

MANUAL REVIEW MAY BE HELPFUL, BUT CAN BE EXPENSIVE

Based on the survey 83% of North American businesses conduct manual reviews, and on an average they review 29% of orders manually. Manual review offers some benefits. As well as helping to weed out fraudulent orders, it can contribute insights into fraud patterns and genuine customer behavior. These insights can be used to fine-tune fraud screening rules and reduce the number of false positives (the number of inadvertent customer insults).

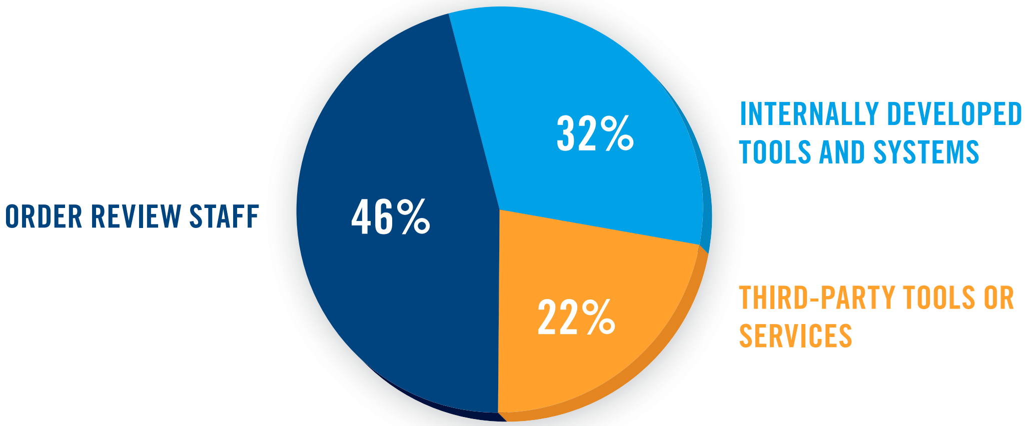
However, manual review is often a costly aspect of fraud management operations: 46% of survey respondents said manual review staff account for the largest single slice of their fraud management budget.

But fraud management budgets are essentially flat. The majority of respondents (61%) expect their budgets for fraud management operations to stay the same over the coming 12 months, and 7% even expect them to decline. It would seem that, for most businesses, there's no money to spare for increased reliance on manual review.

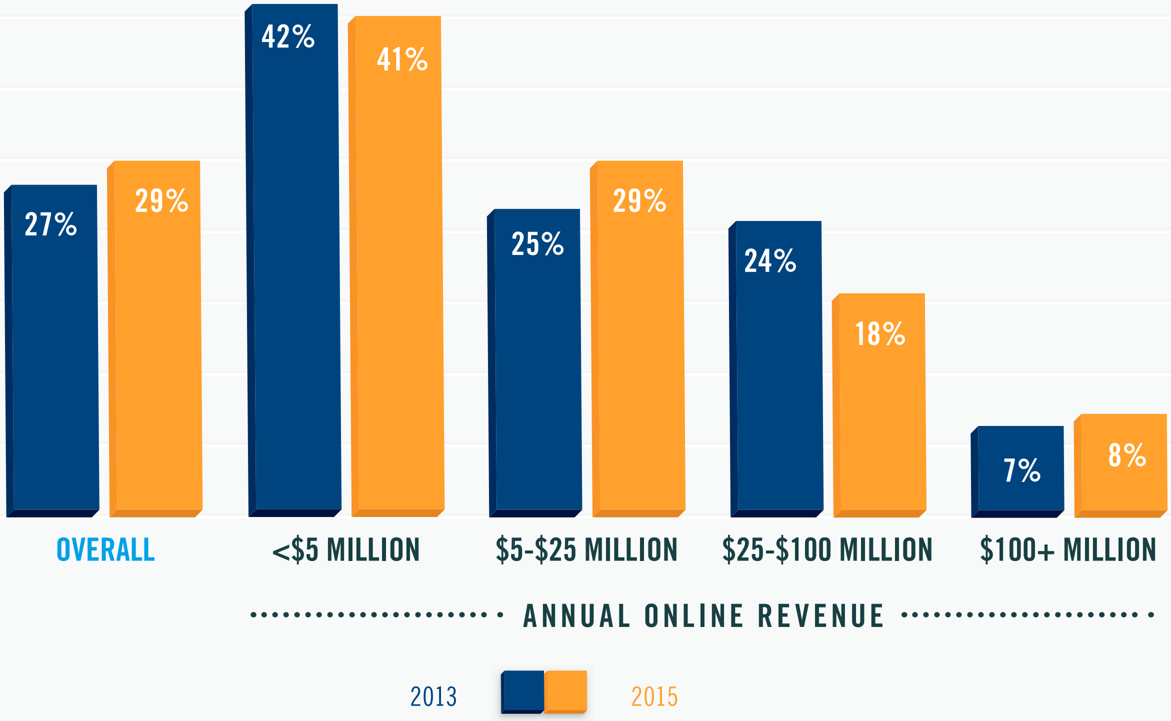
You therefore should make sure you get the very best out of the manual review process. According to our survey, businesses accepted 82% of orders following manual review — an indicator that more orders are being reviewed than is strictly necessary.

When you fine-tune your automated screening processes to optimum effectiveness, it helps produce efficient decisions about more of your orders — leaving only the most ambiguous ones to be investigated manually by your review team.

HOW FRAUD MANAGEMENT BUDGETS ARE SPLIT



MANUAL REVIEW RATES



OPTIMIZING THE MANUAL REVIEW PROCESS

Review teams often account for the largest share of an organization's fraud management budget, so monitoring and optimizing performance is critical. You'll want to consider how the team is performing in the context of your operational goals and in helping to meet your company's overall financial objectives.

1. Drive effectiveness and efficiency by measuring key performance metrics — both by individual reviewer and across the team. Metrics can include:
   - Chargebacks
   - Review times
   - Number of transactions reviewed (if possible)
   - Number of inadvertent customer insults (false positives)
2. Use a work flow automation tool, like CyberSource Decision Manager, that brings together all the information needed to review an order on a single screen, helping team members work more efficiently.
3. Use a case management system to enable a more structured review and gather KPIs (key performance indicators). Measure and review results against overall fraud management KPIs for a specific period of time to determine trends and areas for improvement.
4. Ensure your fraud teams share knowledge about the latest trends and that they understand which information sources / validation databases work best in different markets.

TURNING REVIEWS INTO RULES

At CyberSource, we pay close attention to the orders that our reviewers accept and are confirmed valid, looking for common characteristics such as:

- **PRODUCTS ORDERED**
- **GEOLOCATION ELEMENTS (FOR EXAMPLE, CORRELATING BIN, SHIPPING/BILLING ADDRESS, AND IP LOCATION)**
- **VELOCITY CHARACTERISTICS**
- **DEVICE CONFIGURATION (FOR EXAMPLE, WHETHER FLASH®, JAVASCRIPT®, OR COOKIES ARE ENABLED; BROWSER LANGUAGE; DEVICE CLOCK TIME ZONE)**

We use this analysis to create or amend rules, so that good orders will more likely be automatically accepted in the future, helping to enhance the customer experience.

MANAGING FRAUD IN DIFFERENT CHANNELS

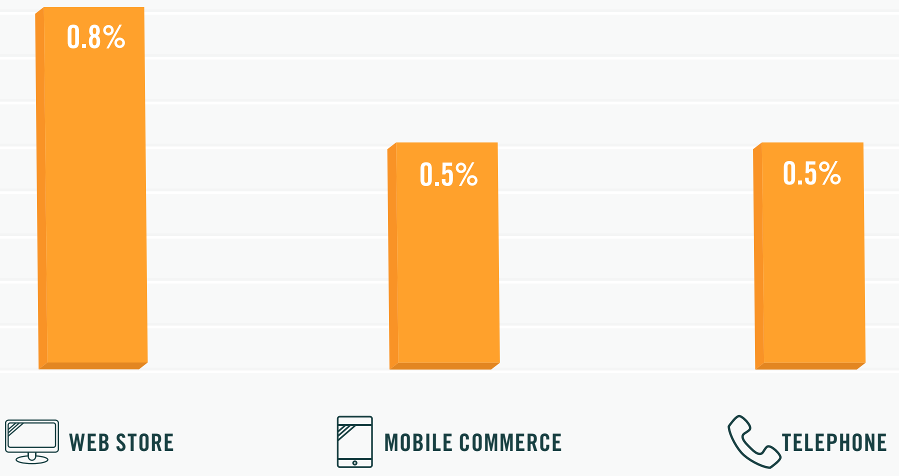
BUSINESSES TRACK FRAUD ACROSS CHANNELS

Of the businesses we surveyed, 62% track fraud losses by order channel. Tracking fraud losses by order channel puts businesses in a better position to tune and improve their fraud management performance in each of the channels they serve.

OVERALL FRAUD LOSS BY ORDER CHANNEL

REPORTED AVERAGE ANNUAL FRAUD LOSS
(EXPRESSED AS % OF ANNUAL REVENUE)

Q: For each of the channel(s) below, what percent of your annual revenue do you expect to lose due to payment fraud?

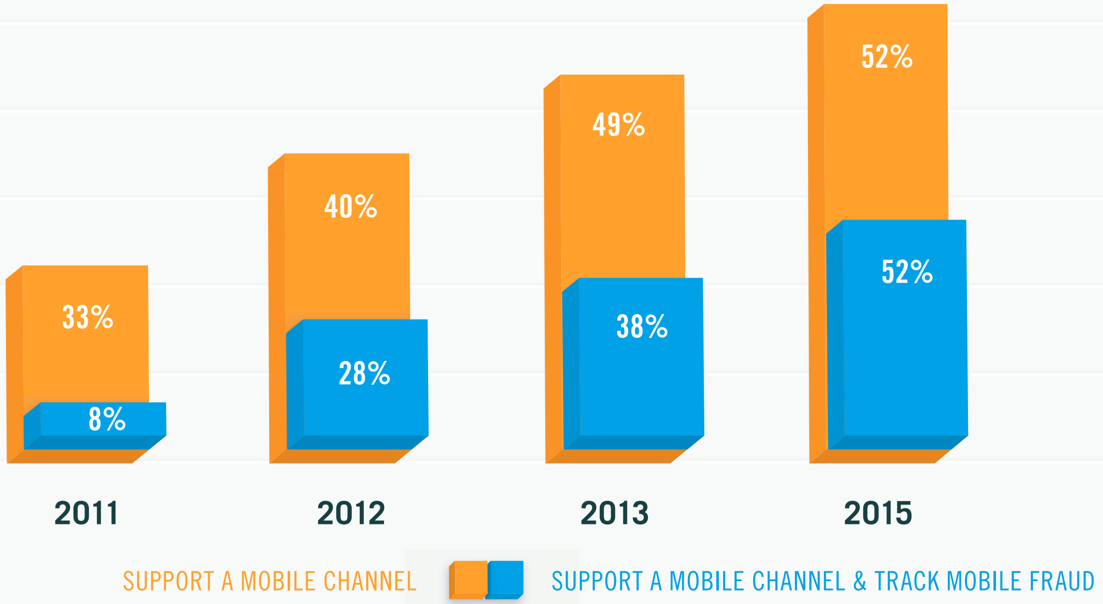


MCOMMERCE IN THE SPOTLIGHT

More businesses than ever are tracking fraud in the mobile channel separately from their web channel.

And as the adoption of the mobile channel has increased, so has the number of respondents who track fraud in that channel. Today, just over half (52%) of respondents offering mCommerce track this channel separately.

GROWTH AND TRACKING OF THE MOBILE CHANNEL



MANAGING MOBILE FRAUD

Although there are many similarities between eCommerce and mCommerce, there are also important differences that are relevant to fraud management. If these differences aren't anticipated, a business may experience higher rates of fraud in the mobile channel than necessary or may reject or review too many genuine mCommerce transactions.

That's why it's important to distinguish between eCommerce and mCommerce from a fraud management perspective and to track them separately — as North American businesses are doing.

Normal customer behavior on a mobile device is often different from normal customer behavior on a PC (a laptop or desktop computer). eCommerce fraud detection rules are designed for typical PC behavior. Whenever mobile behavior differs, these rules may treat perfectly normal behavior as atypical.

All of the information captured about an order — such as the channel, time of day, customer identity, or good purchased — can be used as an input to the tools and rules of fraud management. The more relevant data there is, the more can be done to distinguish genuine from fraudulent transactions.

One powerful piece of data is the device fingerprint, or device ID, giving visibility into the type of device that the order came from. There are good reasons to get as specific as possible with device fingerprinting. For instance, your customer profile, and hence normal customer behavior, may vary significantly across iPhone® and Android™ users. Armed with detailed device information, your fraud management strategies can be even more tailored.

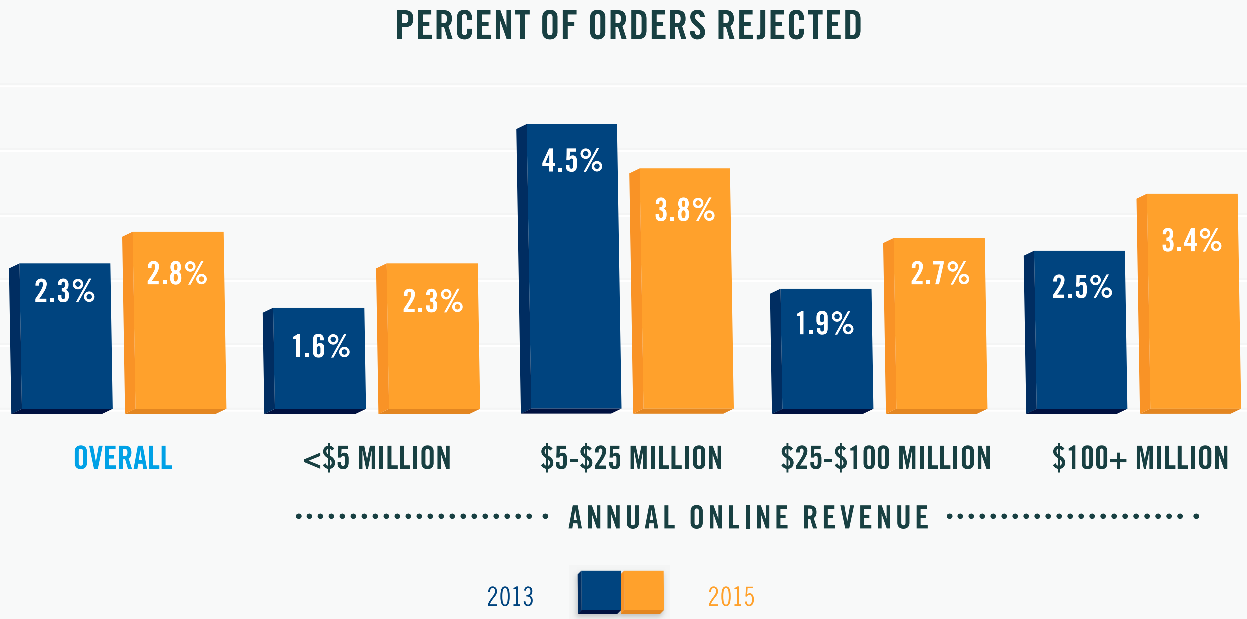
IMPROVING GENUINE ORDER ACCEPTANCE WHILE GUARDING AGAINST FRAUD

REJECTION RATES AND FALSE POSITIVES

More orders were rejected by merchants in 2015 due to suspicion of fraud. North American businesses rejected 2.8% of U.S./Canadian orders due to suspicion of fraud, up from 2.3% last year. A false positive, sometimes referred to as a 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, they can also impact customer loyalty, retention, and sales in the future.

The majority (70%) of survey respondents who track false positives believe that up to 10% of the orders they reject on suspicion of fraud are actually genuine.

ORDER REJECTION TRENDS – BY SIZE OF MERCHANT



INCREASING GENUINE ORDER ACCEPTANCE WITH RULES-BASED PAYER AUTHENTICATION

Implementing payer authentication (3-D Secure) can help you accept more genuine orders. Payer authentication reduces fraudulent activity and lets you benefit from the online payment guarantees offered by major card programs.

Despite the benefits, 3-D Secure introduces an additional security step, which may cause friction for customers and negatively affect conversion rates.

With CyberSource Rules-Based Payer Authentication, you gain control over which transactions are presented for authentication, and which aren't. Rules based on issuer and card holder participation levels can be configured to determine when to authenticate.

Providing a smoother checkout experience for customers can reduce the cart-abandonment rate, while you benefit from the liability shift and interchange savings provided by 3-D Secure.

MANAGING CROSS-BORDER FRAUD

The challenge of distinguishing between fraudulent and genuine customers can be intensified when selling goods or services outside of your domestic market, often due to the lack of local knowledge regarding fraud patterns and what constitutes normal consumer behavior.

Despite the challenges, it is possible to successfully manage fraud risk when handling cross-border transactions, as many North American businesses are demonstrating. Between 2009 and 2011, the fraudulent rate for international orders was more or less static at 2%, but in 2015, it dropped to 0.9%. Although the rate is still approximately 1.5x higher than for domestic orders, the gap is closing (down from 2x in 2012).

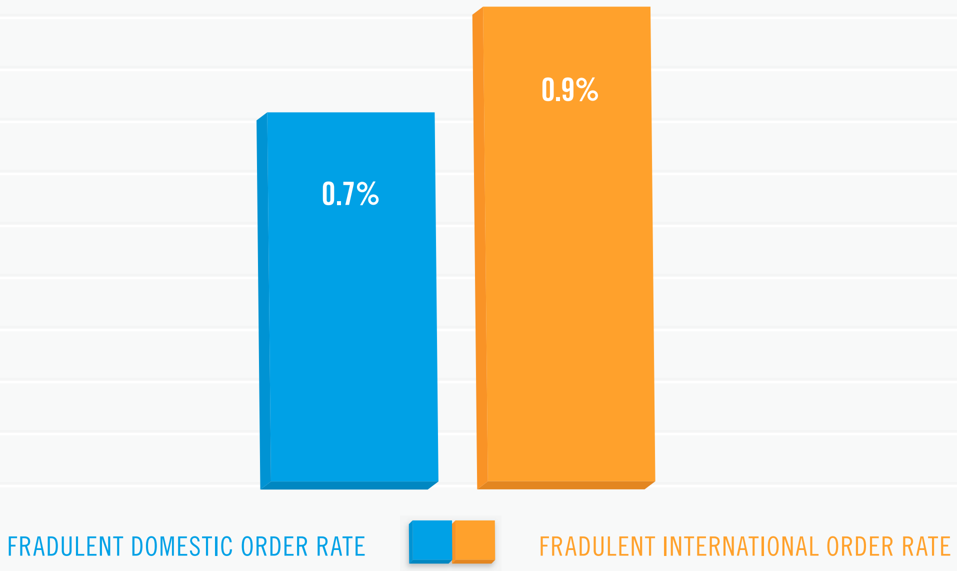
55%

OF U.S. AND CANADIAN BUSINESSES IN THE SURVEY ACCEPT ORDERS FROM OUTSIDE NORTH AMERICA

15%

OF ORDERS ACCEPTED BY U.S. AND CANADIAN BUSINESSES IN THE SURVEY ARE CROSS-BORDER TRANSACTIONS

DOMESTIC AND CROSS-BORDER FRAUD RATES



WORKING WITH A GLOBAL PARTNER

Of all respondents, 44% indicated that they use different fraud strategies when they expand into new geographies.

Businesses should consider the following measures when moving into new geographies:

- Working with sources knowledgeable in local fraud management
- Implementing regionally relevant best practices
- Adjusting fraud scoring rules to reflect the local market

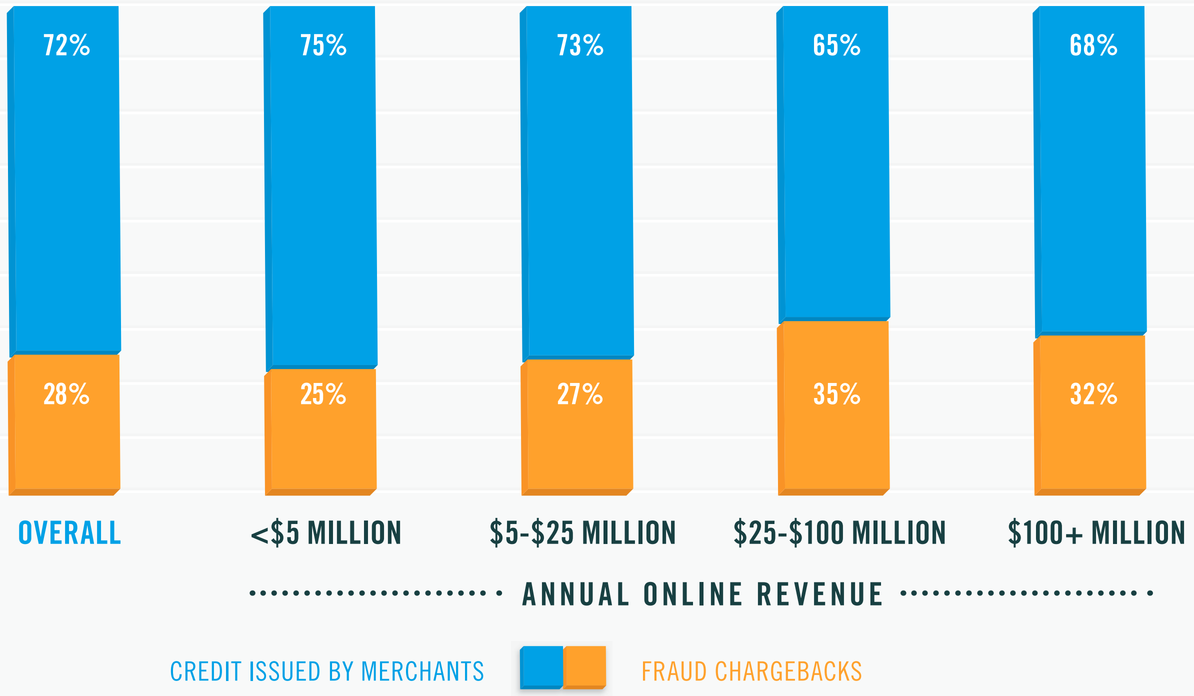
CyberSource can help businesses effectively manage cross-border fraud. We collect fraud data globally and have fraud analyst teams worldwide, including data from 200 countries and territories, analysts on six continents, and region- and country-specific models. We help put this data and expertise to work for our customers to help them address new markets without unnecessarily seeing a spike in fraud rates or possibly turning away genuine customers.

CHARGEBACKS (FRAUD CLAIM MANAGEMENT)

This survey defines fraud losses as fraud-coded chargebacks plus any credits issued by a merchant to customers in response to a fraud claim.

As a result, fraud rates reported tend to be higher than those cited by banks or card networks.

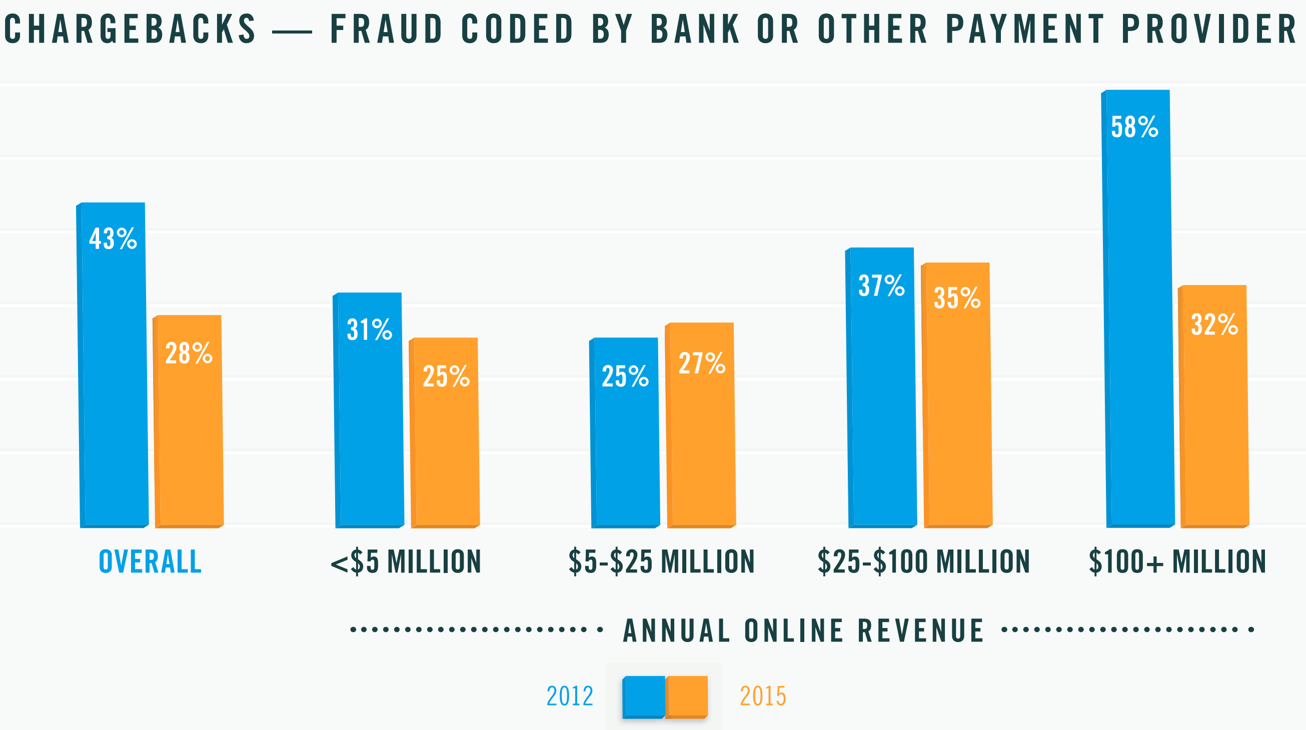
SHARE OF FRAUD CLAIMS



Although chargebacks are the most often cited metric, they account for only 28% of fraud claims, a proportion that has dropped from 43% over a three-year period. It may be that businesses know their existing customers better, because of the trend toward encouraging customers to set up accounts rather than check out as guests. Businesses more often issue credits to regular customers who are known and trusted, in order to maintain goodwill. Although money may be lost in the short term, issuing credits is likely to have a positive effect on relationships with these good customers over the longer term.

Despite the drop in chargebacks as a proportion of fraud rates, the chargeback re-presentment rate (disputed chargebacks) is unchanged since 2013 at 53%, and the win rate (merchants win the challenged chargeback) has declined only slightly over the same period, from 43% to 41%.

CHARGEBACK AS PORTION OF FRAUD



CONCLUSION

The North American businesses in our survey are managing fraud reasonably well, but for optimum effectiveness, fraud reduction must be balanced against the cost of achieving it and the effect on customer acquisition and loyalty. Fraud tactics change constantly as fraudsters try out new ways to circumvent businesses' existing fraud management systems, so what works one month might not work the next.

Automated fraud screening is an efficient means to detect and control fraud. Manual review can provide additional insight, but overreliance on manual review will prove costly.

Fraud management is a challenging balancing act in our increasingly complex and competitive digital economy. But it's a challenge that is addressable. Using the right tools, it is possible to reduce fraud losses and operational costs while improving the customer experience and increasing genuine order acceptance.

HOW CYBERSOURCE CAN HELP

CyberSource provides a complete range of fraud management solutions to help businesses identify fraud faster, more accurately, and with less manual intervention. These include:

CYBERSOURCE ENTERPRISE FRAUD MANAGEMENT

CyberSource offers a multi-layered fraud management solution — from account monitoring to transaction fraud detection, and from rules-tuning to payer authentication — that helps businesses minimize fraud losses, maximize revenue, and minimize operational costs.

Built on intelligence from 68 billion transactions that Visa and CyberSource process annually and proprietary fusion machine-learning algorithms, the CyberSource Enterprise Fraud Management solution represents a comprehensive system that helps you to:

- Protect revenue and operate more efficiently through more accurate, automated detection, reduce fraud losses, and streamline manual review
- Increase sales and maintain customer loyalty by reducing false positives, increasing order acceptance rates, and protecting customer accounts
- Operate with greater flexibility and scalability through confident, real-time control over fraud strategies and access to expert resources and infrastructure worldwide

DECISION MANAGER

CyberSource Decision Manager is the only fraud management platform that uses data from the World's Largest Fraud Detection Radar, increasing fraud visibility more than 200 times — even for top businesses. With Decision Manager, you can create custom rules and models across sales channels and geographies, all with one platform.

DECISION MANAGER REPLAY

With Decision Manager Replay, you can confidently quantify your rule changes before activating them in your live production environment. An industry first, Decision Manager Replay enables you to compare various "what-if" fraud strategies against your historical data, producing a real-time report of likely changes to the transaction disposition and fraud rates.

RULES-BASED PAYER AUTHENTICATION

CyberSource Rules-Based Payer Authentication provides you with control over the customer experience while giving you access to the benefits of liability shift and reduced interchange via 3-D Secure. You can tailor your fraud risk management and decide when to request 3-D Secure authentication, or not to.

ACCOUNT TAKEOVER PROTECTION

Account Takeover Protection actively monitors new account creation and account usage behaviors of online accounts, to help you more accurately distinguish valid from high-risk sessions during account creation, login, and updates. As an extension of Decision Manager, Account Takeover Protection interoperates with the reporting, rules, and tuning tools as part of a fully integrated fraud management platform

MANAGED RISK SERVICES

CyberSource Managed Risk Analysts have deep fraud management experience. Located on six continents, our analysts are able to detect the latest fraud trends quickly to help businesses minimize fraud losses while keeping operations running efficiently.

ABOUT US

CyberSource Corporation, a wholly owned subsidiary of Visa Inc., is a payment management company. More than 400,000 businesses worldwide use CyberSource and Authorize.Net brand solutions to process online payments, streamline fraud management and simplify payment security. The company is headquartered in Foster City, California. CyberSource operates in Europe under agreement with Visa Europe. For more information, please visit www.cybersource.com.

CONTACT CYBERSOURCE

NORTH AMERICA

SAN FRANCISCO, CA, UNITED STATES

T. **+1 888 330 2300**

E. **SALES@CYBERSOURCE.COM**

LATIN AMERICA & THE CARIBBEAN

MIAMI, FL, UNITED STATES

E. **LAC@CYBERSOURCE.COM**

ASIA PACIFIC

SINGAPORE

E. **AP_ENQUIRIES@CYBERSOURCE.COM**

EUROPE, MIDDLE EAST & AFRICA

READING, UNITED KINGDOM

E. **EUROPE@CYBERSOURCE.COM**

For a complete list of worldwide offices, go to: www.cybersource.com/locations