



INSIDE THIS REPORT

PAGES

3	INTRODUCTION
3	MERCHANTS ARE MANAGING FRAUD MORE EFFICIENTLY
3	HOW TO USE THIS BENCHMARK STUDY
4	KEY METRICS
4	FRAUD RATE
5	MANUAL ORDER REVIEW RATE
5	ORDER REJECT RATE
6	FRAUD MANAGEMENT BENCHMARKS
6	THE FRAUD MANAGEMENT PROCESS MODEL
7	AUTOMATED SCREENING
9	MANUAL REVIEW
11	ORDER DISPOSITIONING (ACCEPT/REJECT)
13	FRAUD CLAIM MANAGEMENT
15	SPOTLIGHT ON MOBILE
17	TUNING AND ANALYTICS
19	CONCLUSION
20	CYBERSOURCE FRAUD MANAGEMENT SOLUTIONS
20	CYBERSOURCE DECISION MANAGER
21	MANAGED RISK SERVICES
21	RULES-BASED PAYER AUTHENTICATION
21	VERIFICATION AND COMPLIANCE SERVICES
22	ABOUT THE SURVEY

INTRODUCTION



MERCHANTS ARE MANAGING FRAUD MORE EFFICIENTLY



CyberSource sponsors annual surveys that look at how merchants are managing fraud in their online channels, including both eCommerce and mCommerce.

The 15th annual survey shows that merchants are managing fraud more efficiently. North America is a mature eCommerce market and trends have been fairly stable over the past few years. This year's metrics show marked improvements in key areas:

The majority of merchants have improved order conversion. They are experiencing lower rates of order rejection while keeping fraud losses stable—meaning there are fewer ‘customer insults’.

In the increasingly important mCommerce channel, merchants are paying greater attention to managing mobile fraud and are achieving good results.

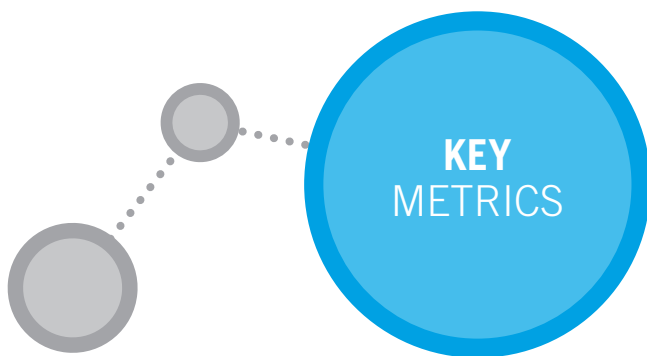
HOW TO USE THIS BENCHMARK STUDY

We've published results from our 15th annual survey of fraud management practices in this Benchmark Study to help merchants gauge their performance against peer organizations, and understand where to focus and invest for future improvement. The study also provides an overview of long-term trends and indicators of emerging challenges in the fraud management space.



IN THIS STUDY YOU'LL FIND

- A summary of key metrics
- Benchmarks for each stage in the fraud management process flow
- Conclusions based on the survey findings
- An overview of CyberSource's fraud management solutions



FRAUD RATE

North American merchants continue to manage fraud efficiently, with the rate of eCommerce revenue lost to fraud remaining at the same low rate since 2010.

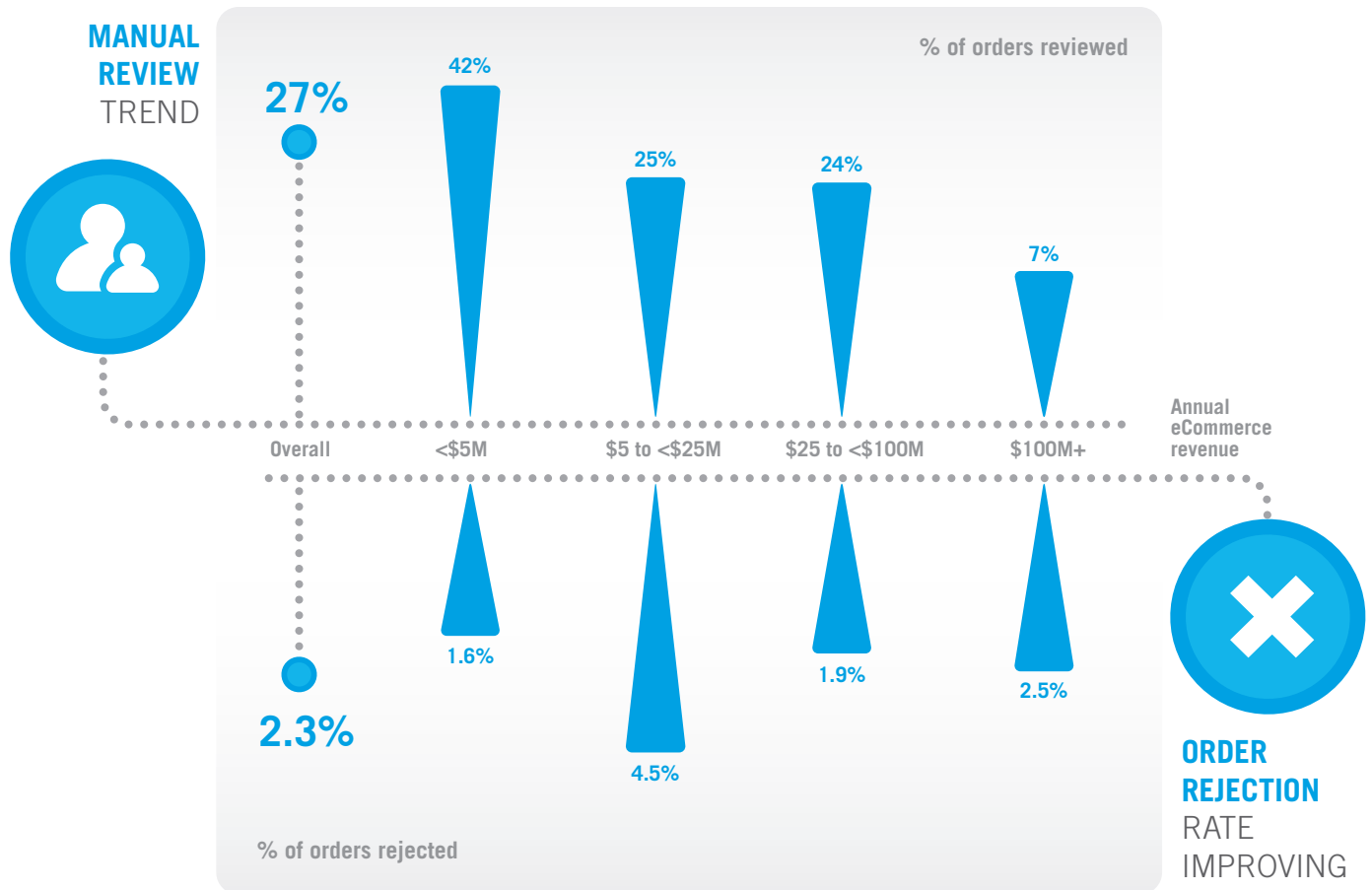


1/4

ORDERS MANUALLY
REVIEWED

MANUAL ORDER REVIEW RATE

The proportion of orders merchants review manually for fraud has remained steady at around one in four overall. The largest merchants apply manual screening to less than one in 10 orders, while the smallest review two out of every five.



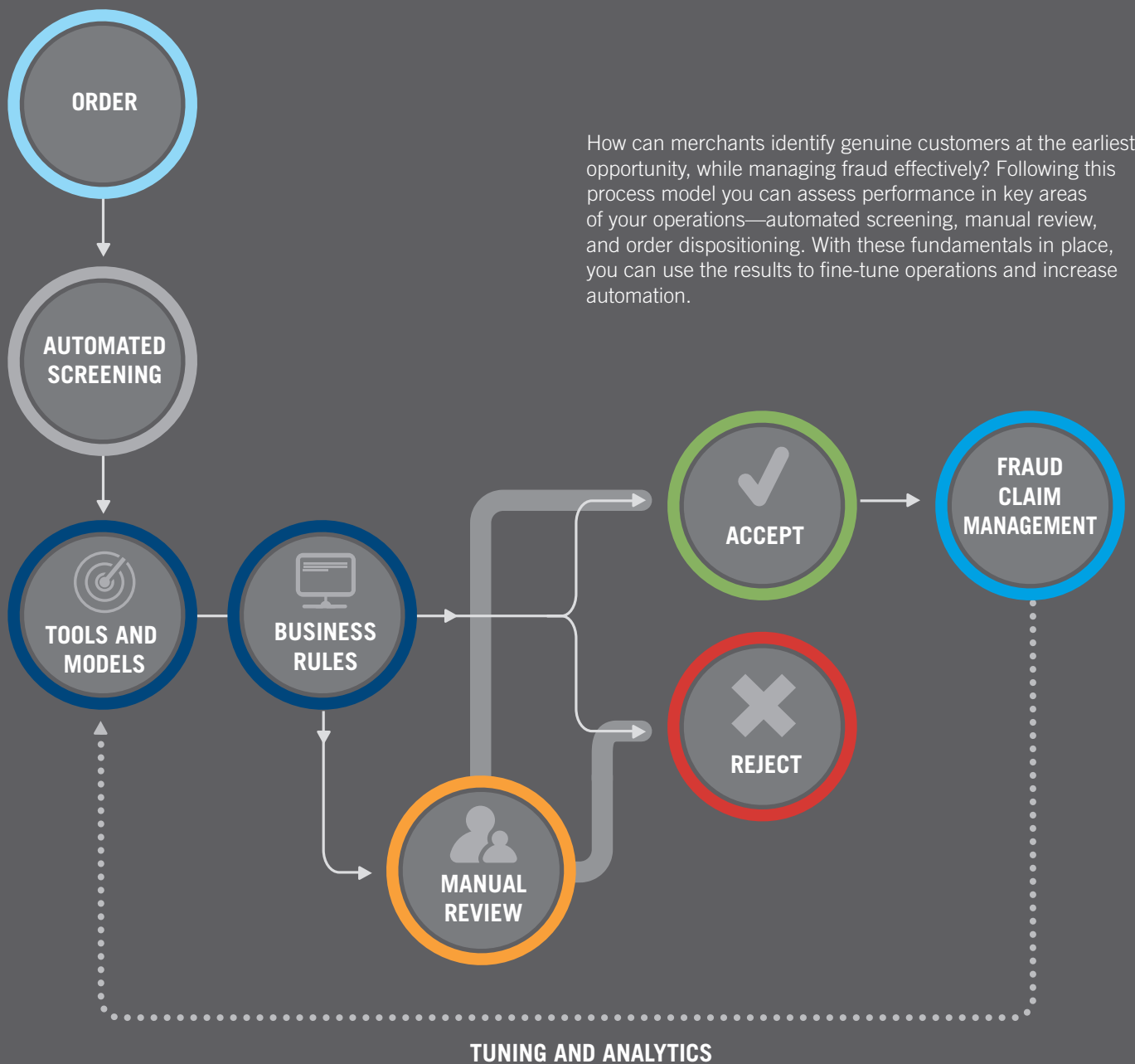
ORDER REJECT RATE

Overall, merchants have improved order conversion and reduced order rejection rates. They have achieved this while holding fraud losses stable, which implies fewer customer insults.

2.3%

OF ORDERS REJECTED

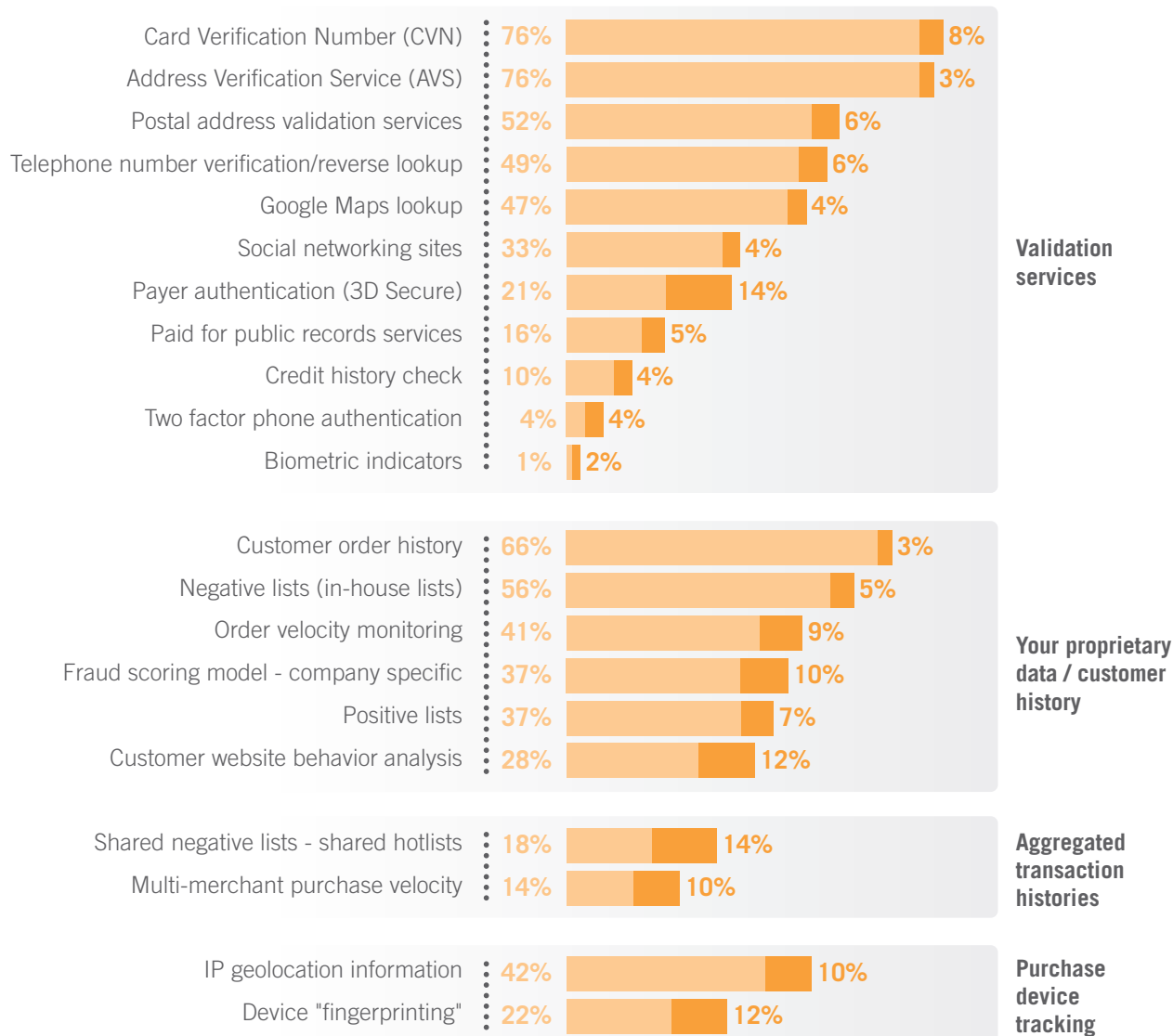
FRAUD MANAGEMENT BENCHMARKS



AUTOMATED SCREENING

During the automated screening process, a rules-based system and risk evaluation are typically applied to determine the likelihood of fraud. An effective automated screening process, based on a wide-ranging fraud management solution such as CyberSource Decision Manager, will deliver rapid, accurate and efficient decisions about the majority of orders, leaving only the most suspicious orders for the review team to investigate manually.

MOST ADOPTED FRAUD DETECTION TOOLS



The two most adopted screening tools, Card Verification Number (CVN) and Address Verification Service (AVS), are also rated among the six most effective. Screening an order against a customer's order history is the most adopted screening tool that relies on a merchant's own data, and is also rated among the top six for effectiveness.

Tools like Google Maps and IP geolocation information are becoming more popular. They can reveal, for example, that an order is being placed from an address that is actually an empty lot, raising a red flag. Other emerging tools, such as device fingerprinting and website behavior analysis, are also attracting a lot of interest from merchants.

By using a commercial fraud management system like CyberSource Decision Manager, merchants gain access to a spectrum of tools, ranging from those that have proved themselves over the long term to newer tools like device fingerprinting. Additionally, some systems like Decision Manager also permit the passing of custom data elements through the API to further tailor evaluation for the specific business. These systems also provide tools that enable weighting of individual rules and the scoring model to customize fit to different businesses.

DEVICE FINGERPRINTING



Device fingerprinting is worth looking at more closely, as 55% of merchants using it rate as one of their most effective tools—a rating that only company-specific fraud scoring models comes close to. Device fingerprinting is a simple way to improve order acceptance rates and recognize returning customers, especially when it is integrated into a broader screening strategy. Given its effectiveness, the percentage of merchants currently using device fingerprinting (22%) seems surprisingly low; but 12% say they planned to implement it.

TOP 3 TOOL FOR

55%

OF MERCHANTS

TACKLING CLEAN FRAUD

A major issue that has emerged over recent years is 'clean fraud'. It is becoming much more difficult to distinguish valid orders from fraudulent orders as fraudsters become more sophisticated.

Merchants need to apply more data to identify the subtle indicators of fraud—but relying on your own data may not be enough to do this effectively. Aggregated into the equation can make the task more achievable and help merchants identify new fraud patterns as they emerge. Tools such as device fingerprinting and behavior analysis that address non-payment-related aspects of an order will also help merchants address clean fraud.



81%

OF MERCHANTS
PERFORM
MANUAL REVIEWS

27%

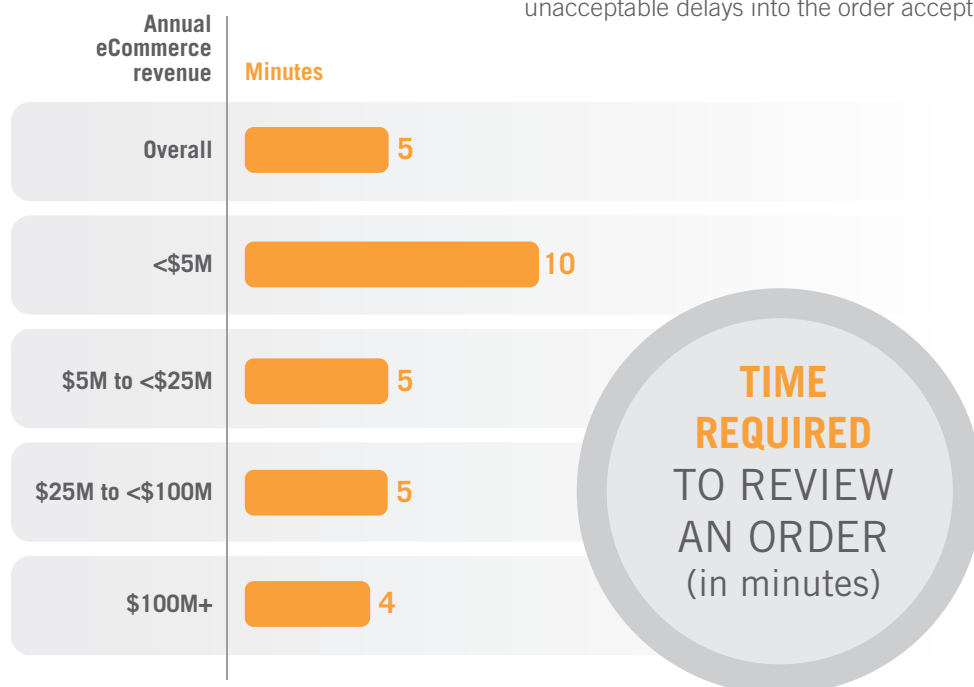
OF ORDERS ARE
REVIEWED MANUALLY

MANUAL REVIEW

After evaluation by an automated screen process, orders with more ambiguous transaction characteristics will be sent for deeper investigation by a review team. The team will use additional data verification sources and apply their own judgment—developed through experience—to make a decision.

The proportion of North American merchants performing manual reviews of eCommerce orders, and the percentage of orders subject to review, have remained stable over the past five years, despite growth in eCommerce volumes.

Larger merchants review a lower percentage of orders than smaller merchants do. This may be because they have deployed more effective automated screening tools, so fewer orders get passed to manual review teams. However, despite the largest merchants' low review rate of less than 10%, the sheer volume of orders they handle still means they need to employ sizeable review teams to do the work quickly and efficiently enough to avoid introducing unacceptable delays into the order acceptance process.



Overall, merchants typically spend five minutes manually reviewing a suspicious order, a time frame that hasn't changed since 2012. Smaller merchants have got faster at manual reviews, with a median of 10 minutes currently compared to 15 minutes in the past.



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 workflow 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. 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.



TURN 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:



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.

2.3%

OF ORDERS REJECTED

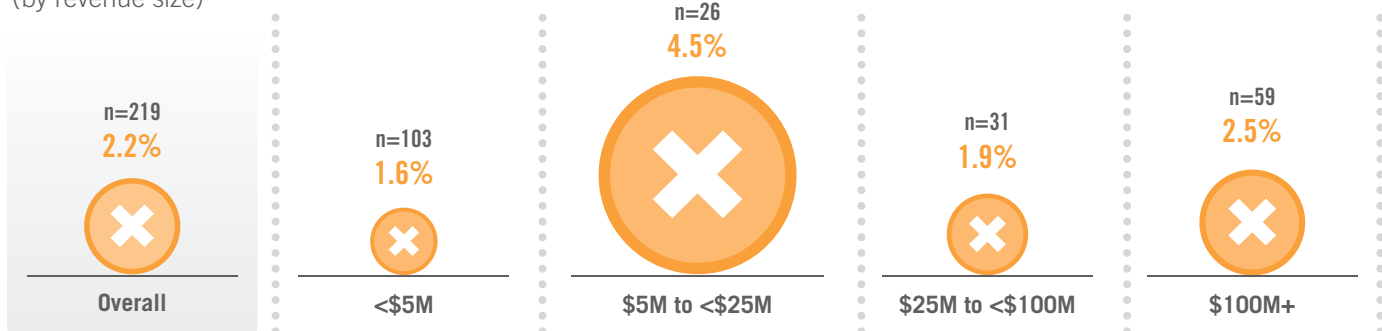
ORDER DISPOSITIONING (ACCEPT/REJECT)

Following automated screening and, if necessary, manual review, the decision will be made whether to accept or reject an order. Examining post-manual review acceptance and rejection levels will be especially valuable in helping merchants tune their automated screening systems and make best use of their manual review teams.

Merchants of all sizes have improved order conversion and reduced order rejection rates. They have achieved this while holding fraud losses stable, which implies fewer customer insults.

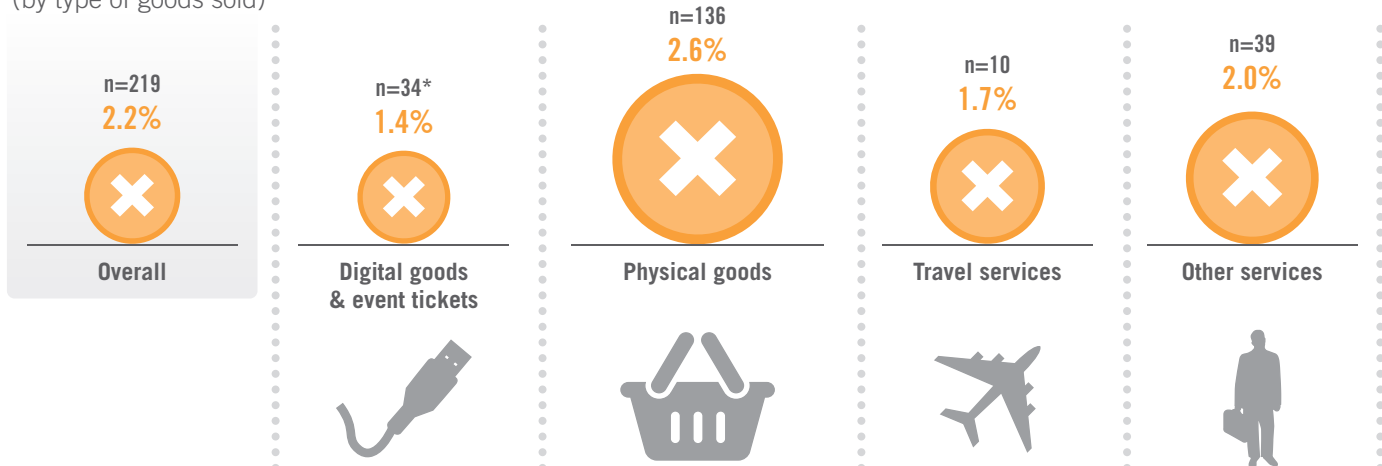
PERCENT OF ORDERS REJECTED

(by revenue size)



PERCENT OF ORDERS REJECTED

(by type of goods sold)



Physical goods retailers reject slightly more orders on suspicion of fraud than merchants selling other types of goods and services. This is probably because a fraudulent order typically costs them more, owing to the higher cost of the goods sold plus the shipping costs that other types of merchant are not as exposed to. As a result, physical goods retailers are slightly more risk averse.

10%

FALSE POSITIVES

Fifty-three percent of merchants track the rate at which valid orders are rejected. Over 70% believe that up to 10% of rejected orders are actually valid.



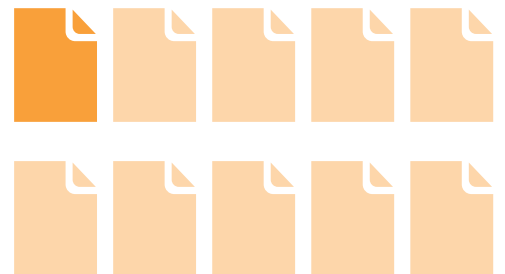
53%
**TRACK
ORDER
REJECTION**



MOST MERCHANTS (>70%)

BELIEVE UP TO

10%
**OF REJECTED
ORDERS ARE VALID**



Eighty-five percent of the orders merchants review manually are accepted. This implies there is room for improvement or refinement of many merchants' automated screening process—perhaps by analyzing data for fraud patterns on an ongoing basis and tuning screening rules to try and accept more orders while holding or reducing risk/fraud rates—in order to reduce the number of orders that are passed for manual review and help maximize the productivity of those teams.

Sixty-eight percent of the merchants surveyed track the fraud rate of their manually reviewed orders, and say that 3% of orders accepted post-manual review later turn out to be fraudulent. This rate has improved slightly over the past three years, indicating the effectiveness of manual review teams.

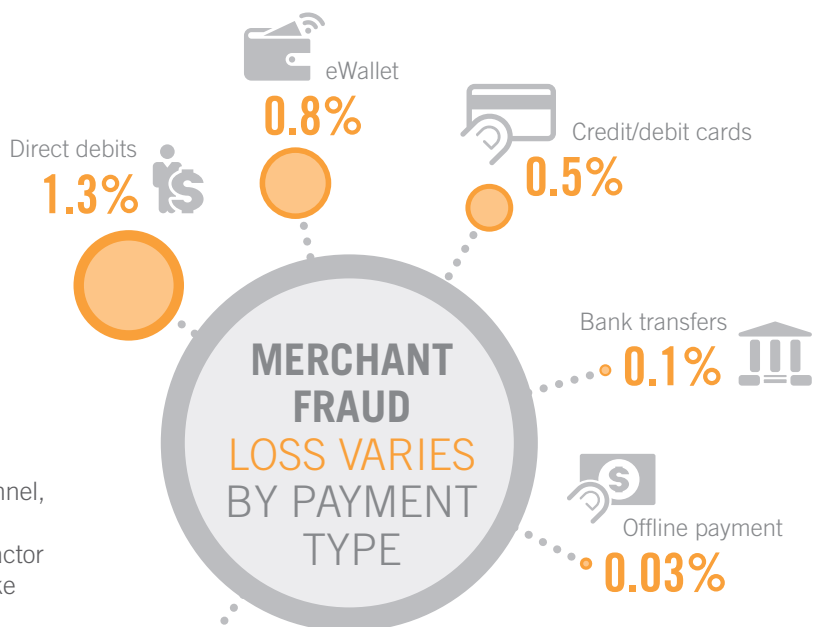
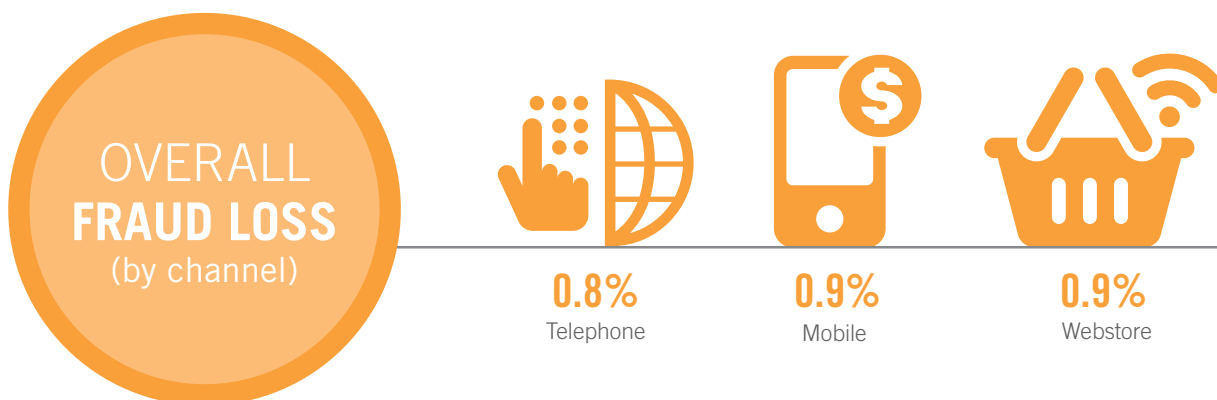
85%

**OF ORDERS ACCEPTED
AFTER MANUAL REVIEW**



FRAUD CLAIM MANAGEMENT

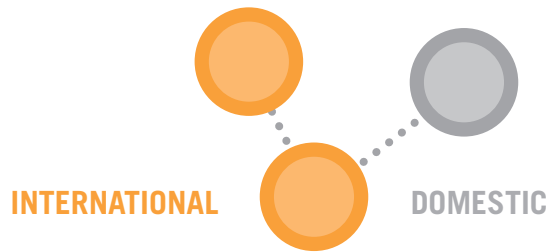
We define fraud as fraud coded chargebacks and also any credits issued by a merchant to customers in response to a fraud claim. As a result, actual fraud rates reported tend to be higher than those cited by banks or card networks.



As well as varying by channel, fraud losses also vary by payment type—another factor merchants will want to take into account when tuning their fraud management systems.

INTERNATIONAL FRAUDULENT ORDER RATE

2X
DOMESTIC



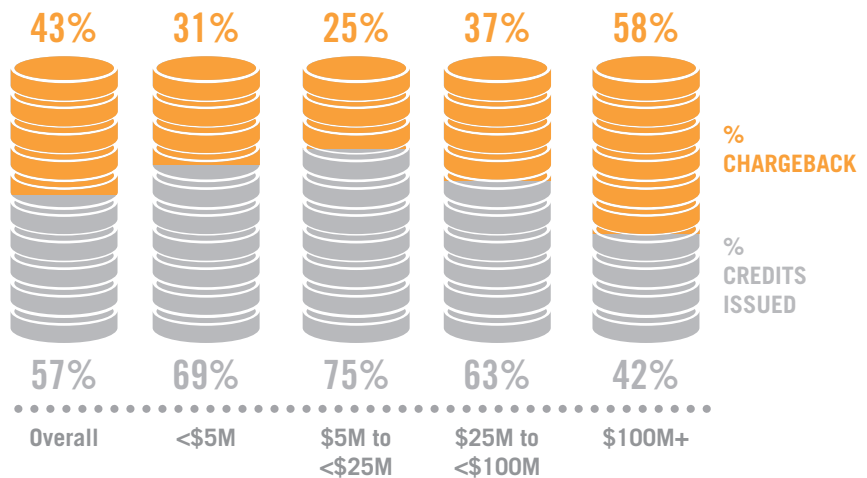
Orders from outside North America have a higher risk of being fraudulent—fraud loss rates on these orders are 2X domestic rates.

AROUND

50%
OF FRAUD CLAIMS
ARE CHARGEBACKS

Although chargebacks are the most often cited metric, they account for only 43% of all fraud claims, a proportion that has been consistent for several years.

CHARGEBACKS ONLY PORTION OF FRAUD LOSS

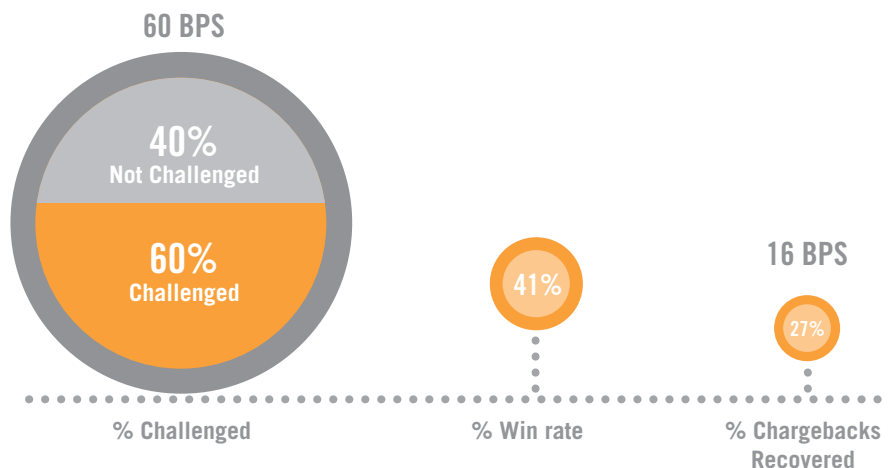


41%

WIN RATE ON CHARGEBACK RE-PRESENTMENT

On average 41% of the time merchants 'win' the re-presentment, resulting in recovery of around one in four fraud chargebacks by merchants.

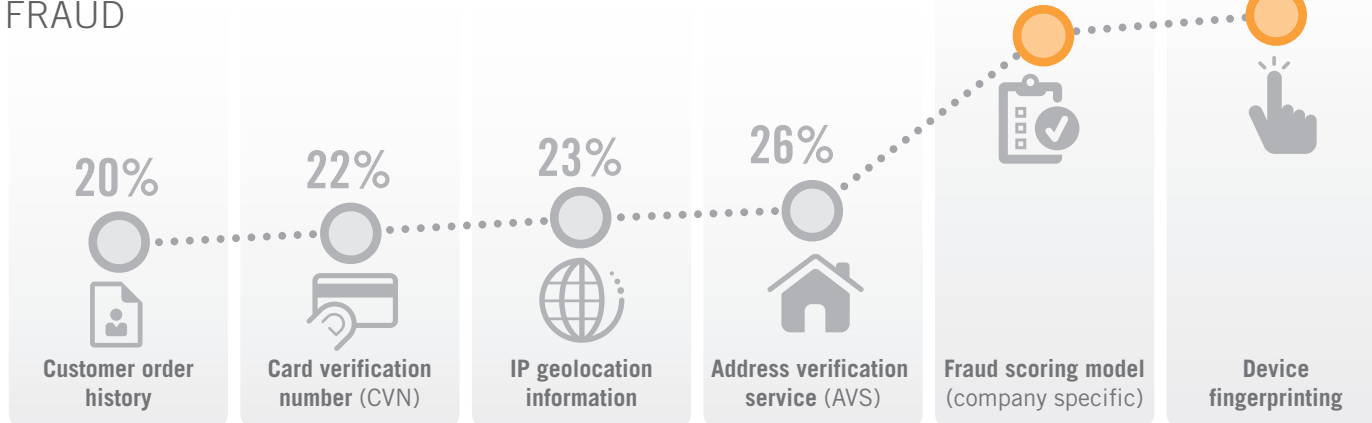
CHARGEBACK RE-PRESENTMENT



SPOTLIGHT ON MOBILE

The mobile channel is seeing increasing adoption by merchants—just under half the merchants in our survey have an mCommerce operation. Merchants must tune their fraud management processes and systems to track and manage mobile fraud risk, as specific challenges and characteristics are associated with it. Overall, merchants that do give mobile fraud management the attention it requires are achieving good results.

MOST EFFECTIVE TOOLS FOR MANAGING MCOMMERCE FRAUD



% Using Selecting as Most Effective

CHARGEBACK RATE BY MOBILE ENVIRONMENT

	Browser	Application
Average	0.59	0.28
Median	0.37	0.01
Total Responses	102	99
Track	16%	12%
DK	43%	44%
DT	41%	43%
DK/DT	84%	88%

n | Browser: 15 / Application: 12

Note: The majority of merchants with a mobile channel were unable to report their fraud chargeback rate for this channel, as they do not tag chargeback data with order channel information.

MOBILE FRAUD PERCEPTION GENERAL



5% Significantly lower than eCommerce

39%

No different than eCommerce

23% Significantly higher than eCommerce

32%

Don't know

13

95

55

78



of respondents

241

Note: contrary to this perception... our quantitative surveys and experience show that, merchants who actually track and manage mobile fraud—distinct from eCommerce—typically manage mobile fraud rates to equal or lower rates than those of eCommerce.



Merchants additionally perceive there are different levels of risk associated with different mobile operating systems.



"Mobile is still new to us but we are finding as much as 70% of new customers are using mobile."

"There are more commonly typos in a mobile order."

"Mobile consumers are more impatient with false positives."

"Mobile is harder to track via IP address—different WiFi and hotspots mean different IP addresses."

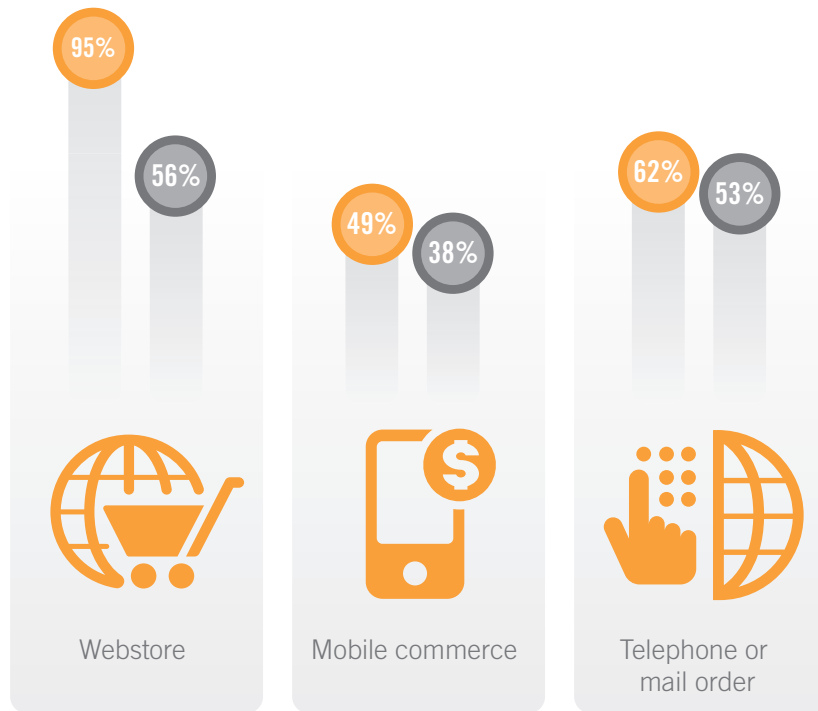
"We currently don't differentiate between mCommerce and eCommerce. However, we believe it is a growing channel and plan to isolate the data in 2014 to have better tracking."

TUNING AND ANALYTICS

Evolving fraud patterns and techniques, emerging fraud management tools, and learnings from fraud tracking efforts are all factors merchants will need to take into account when tuning their fraud management processes for maximum efficiency.

MERCHANTS TRACKING FRAUD BY CHANNEL

% Support order channel
% Track fraud for channel



Only about half of North American merchants track fraud losses by order channel, but if merchants don't collect this information, they may struggle to measure or improve their performance. In addition, different channels provide different types of information about orders. A fraud management tool like CyberSource Decision Manager lets you build and tune risk rules based on which channel an order comes from, so that you can take advantage of the channel-specific information that's available.

TOP 10 PERCEIVED FRAUD THREATS

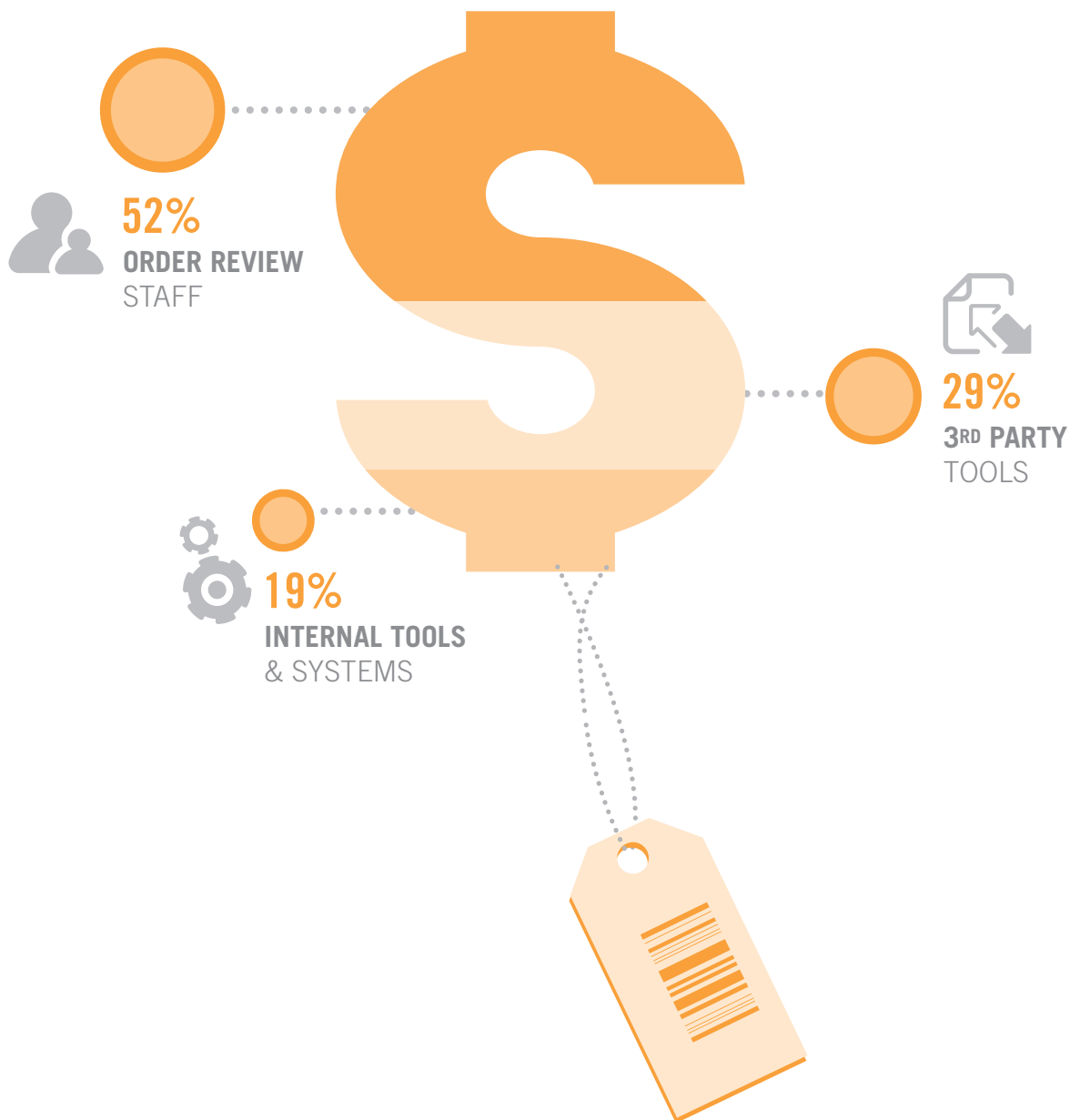
Regardless of size, merchants rank the top 10 types of fraud threat in much the same order. The only notable exception is that the largest merchants put phishing/pharming/whaling at the top of the list, and triangulation schemes closer to the middle.

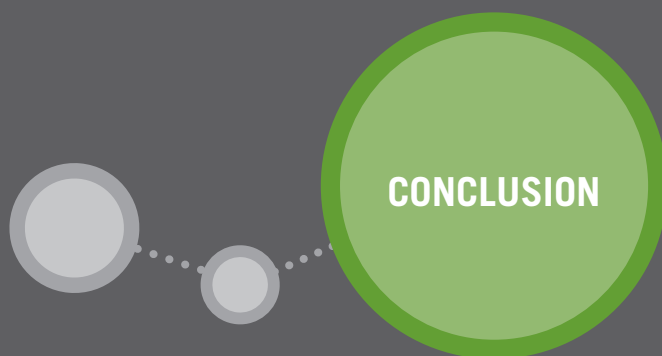


FRAUD MANAGEMENT SPENDING ALLOCATION

Merchants typically spend slightly over half their fraud budget on the manual order review team—a proportion that has been stable for a number of years. It's important to invest in systems that make manual review teams as efficient and productive as possible, to help scale fraud management efforts as eCommerce volumes increase.

AVERAGE % SPENDING ALLOCATION FOR FRAUD MANAGEMENT





The findings from our 15th annual survey indicated that North American merchants are managing fraud efficiently, with a lower order rejection rate at the same fraud rate.

During the period studied merchants:

- **KEPT FRAUD LOSSES UNDER CONTROL**
- **IMPROVED ORDER CONVERSION**
- **REJECTED FEWER VALID CUSTOMER ORDERS, MEANING THERE WERE FEWER CUSTOMER INSULTS**



FRAUD RATE



MANUAL REVIEW RATE



REJECT RATE

Manual order review—using people to help combat fraud threats—was still an important element of the fraud management process, and this is likely to continue. To help scale fraud management efforts as eCommerce volumes increase, merchants need to focus their efforts on improving their automated screening systems. That way, fewer orders will be passed to the review team, enabling them to focus their efforts on the most suspicious orders and improve their productivity and effectiveness.

TO THIS END, MERCHANTS MAY WANT TO CONSIDER:

- Integrating newer tools, such as device fingerprinting
- Tuning their tools and systems to take account of different threats and characteristics in different channels
- Using the results of manual order reviews to build new business rules or amend existing rules



CYBERSOURCE PROVIDES A COMPLETE RANGE OF FRAUD MANAGEMENT SOLUTIONS. THESE INCLUDE ONE OF THE WORLD'S LEADING FRAUD MANAGEMENT SYSTEMS, TRAINING, CONSULTATION, ACTIVE MANAGEMENT OF FRAUD SCREENING, AND OPTIONS FOR OUTSOURCING ALL OR PART OF YOUR FRAUD MANAGEMENT OPERATIONS.

CYBERSOURCE DECISION MANAGER

Our global fraud management portal, Decision Manager, features the **WORLD'S LARGEST FRAUD DETECTION RADAR**. It provides the capability for a merchant to increase fraud detection accuracy, and automate and streamline fraud management operations. With Decision Manager merchants get more information about their inbound orders, and can analyze them against data generated from the more than 60 billion transactions that Visa and CyberSource process annually. Decision Manager enables merchants to **increase their fraud pattern visibility up to 200X**, or more.

- **Access 260+ global validation tests and services**
- **Use a powerful business user rule management interface**
- **Benefit from a flexible case management system**
- **Powerful analytics including Decision Manager Replay to test new rule performance**

1



DECISION MANAGER'S 260+ GLOBAL VALIDATION TESTS AND SERVICES INCLUDE:

- Device fingerprinting with packet signature inspection
- IP geolocation
- Velocity monitoring
- Aggregated transaction histories
- Neural net risk detection
- Positive/negative/review lists
- Global telephone number validation
- Global delivery address verification services
- Standard card brand services (AVS, CVN)
- Custom fields for your own data

2

MANAGED RISK SERVICES

CyberSource Managed Risk Services combines Decision Manager with the services of our expert personnel to assist your fraud management operation. We work with you to define your requirements, then design and implement a solution tailored to meet your business goals.

Our analysts have deep fraud management experience in your industry. With a global staff on six continents, our analysts are able to detect the latest fraud trends quickly to help minimize your fraud losses while keeping your operations running efficiently. Our multi-lingual review team can provide your business with 24/7 risk screening capability. Rigorous ongoing training and performance monitoring of our fraud team helps ensure consistently high quality service.

RULES-BASED PAYER AUTHENTICATION



3

Rules-Based Payer Authentication helps you enjoy the fraud liability shift benefits of 3D Secure services and reduce the risk of checkout abandonment. You configure rules to determine when you present authentication to your customers and when you don't. Supported 3D Secure programs include Verified by Visa, MasterCard® SecureCode™, American Express SafeKey®, and JCB J-Secure.

VERIFICATION AND COMPLIANCE SERVICES

CyberSource provides verification and compliance services that helps businesses to:

4

- **VERIFY SPECIFIC CUSTOMER DATA DURING NON-FACE-TO-FACE TRANSACTIONS**
- **USE ADDITIONAL DATA POINTS FOR FRAUD DETECTION**
- **COMPLY WITH GOVERNMENT POLICIES AND TAX LAWS**
- **COMPLY WITH THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)**

ABOUT THE SURVEY

The benchmarks in this study are based on an in-depth survey of 347 merchants of all sizes and from a variety of sectors throughout the US and Canada.

The merchant sample represents approximately **\$1 out of every \$9** spent online by consumers in survey year - equating to **approximately 12% of global eCommerce revenues.***

1:9\$ 12%

**Using eMarketer's global estimate for B2C eCommerce.*



59%

Physical goods



18%

Digital goods



18%

Other services



5%

Travel services

TYPE OF MERCHANT

SIZE OF MERCHANT (Annual eCommerce Revenue)

46%

<\$5M

13%

\$5M to \$25M

17%

\$25M to \$100M

24%

\$100M+



CyberSource®

CyberSource is a global payment management company and an industry leader in fraud management solutions. Our solutions help businesses improve profitability by detecting fraud sooner and more accurately, and by streamlining fraud management operations.

CyberSource has been providing fraud management tools since 1995, and today offers solutions and support spanning the entire payment workflow, integrating risk management with global and alternative payments on a single platform.

We operate globally with teams of fraud analysts and advisors in over a dozen locations around the world. Our systems and services screen orders originating from over 200 countries and, because we are a Visa company, we are able to build insights on what is arguably the world's largest repository of transaction data.

We have been researching fraud trends and practices for many years in various parts of the world—including 15 years in North America—and in key vertical market sectors. In addition to this study that focuses on North America, we also publish benchmark studies for Latin America, the UK and France, and for the online travel sector.



CONTACT CYBERSOURCE

NORTH AMERICA

San Francisco, CA, United States

t. +1 888 330 2300

t. +1 650 432 7350

e. sales@cybersource.com

LATIN AMERICA & THE CARIBBEAN

Miami, FL, United States

t. + 1 305 328 1998 (Miami)

t. + (52 55) 5387 4185 (Mexico)

t. + 55 11 2102 0088 (Brazil)

e. lac@cybersource.com

ASIA PACIFIC

Singapore

t. + 001 800 6671 5000 (Singapore / Thailand)

t. + 00 800 6671 5000 (Malaysia)

t. + 000 800 630 1003 (India)

t. + 1 800 8 756 8388 (Philippines-Globe)

t. + 1 800 10 802 7222 (Philippines-PLDT)

t. + 86 21 6109 5141 (Greater China)

t. + 0011 800 6671 5000 (Australia)

t. + 00 800 6671 5000 (New Zealand)

e. ap_enquiries@cybersource.com

EUROPE, MIDDLE EAST & AFRICA

Reading, United Kingdom

t. + 44 (0) 118 990 7300 (UK & Spain)

t. + 33 170 98 32 20 (France)

t. + 971 4 457 7200 (Middle East & North Africa)

t. + 7 (495) 787 4140 (Russia)

t. + 44 (0) 203 684 5690 (Sub-Saharan Africa)

e. europa@cybersource.com

JAPAN

Tokyo, Japan

t. + (03) 3548 9873

e. sales@cybersource.co.jp